

AOS-CX 10.14 Command-Line Interface Guide

9300, 9300S Switch Series



**Hewlett Packard
Enterprise**

Published: November 2025

Version: 1

Copyright Information

© Copyright 2025 Hewlett Packard Enterprise Development LP.

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America.



Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Bluetooth is a trademark owned by its proprietor and used by Hewlett Packard Enterprise under license.

About this document	48
Applicable products	48
What's new in this release	48
Latest version available online	51
Command syntax notation conventions	51
About the examples	52
Identifying switch ports and interfaces	53
Introduction to the AOS-CX CLI	54
CLI access	54
Getting CLI help	54
Authority levels	55
Command contexts	56
Operator context (>)	56
Navigating to the operator context (>)	56
Auditor context	56
Manager context (#)	57
Navigating to the manager context (#)	57
Global configuration context (config)	57
Navigating to the config context	58
Other configuration command contexts	58
Support for range contexts	59
Rules for range contexts	61
Command history	61
Command completion	62
Pipe () support in show commands	62
Command syntax notation conventions	63
Service OS CLI commands	64
boot	64
cat	64
cd path	65
config-clear	66
cp	66
du	68
erase zeroize	69
exit	70
format	71
identify	72
ip	72
ls	73
md5sum	75
mkdir	76
mount	77
mv	78
password (svos)	78
ping	79
pwd	80
reboot	81

rm	81
rmdir	82
secure-mode	83
sh	84
system serviceos password-prompt	85
umount	86
update	87
tftp	88
version	89
ACL commands	91
ACL application	91
access-list copy	92
access-list ip	96
access-list ipv6	107
access-list log-timer	115
access-list mac	118
access-list resequence	124
access-list reset	126
access-list secure-update	130
apply access-list control-plane	131
apply access-list (to interface or LAG)	132
apply access-list (to interface VLAN)	134
apply access-list (to subinterface)	136
apply access-list (to VLAN)	138
clear access-list hitcounts	140
clear access-list hitcounts control-plane	142
object-group address resequence	142
object-group address reset	143
object-group all reset	144
object-group ip address	145
object-group ipv6 address	147
object-group port	149
object-group port resequence	151
object-group port reset	152
show access-list	153
show access-list control-plane	158
show access-list hitcounts	160
show access-list hitcounts control-plane	163
show access-list secure-update	164
show capacities	165
show capacities-status	167
show object-group	170
ACL and Policy hardware resource commands	173
show resources	173
ARP commands	175
arp ip	175
arp process-grat-arp	176
clear arp	177
ip local-proxy-arp	178
ip proxy-arp	179
ipv6 local-proxy-nd	180
ipv6 neighbor mac	181
show arp	182

show arp state	183
show arp summary	184
show arp timeout	186
show arp vrf	187
show ipv6 neighbors	188
show ipv6 neighbors state	189
HPE Aruba Networking Central commands	191
hpe-anw-central	191
hpe-anw-central support-mode	192
configuration-lockout central managed	192
diag-dump rest basic	194
disable	195
enable	195
location-override	196
location-override-alternative	198
show hpe-anw-central	199
show running-config current-context	203
Banner commands	204
banner	204
show banner	205
BFD Commands	207
bfd	207
bfd <IPV4-ADDR>	207
bfd all-interfaces	208
bfd detect-multiplier	209
bfd disable	210
bfd enable (Context: config-hsc)	211
bfd disable (Context: config-hsc)	212
bfd echo disable	212
bfd min-echo-receive-interval	213
bfd min-receive-interval	214
bfd min-transmit-interval	215
clear bfd statistics	217
ip ospf bfd	217
ip ospf bfd disable	218
ip route bfd	219
ipv6 ospfv3 bfd	220
ipv6 ospfv3 bfd disable	221
neighbor fall-over bfd	222
ospfv3-af ipv4 bfd	223
ospfv3-af ipv6 bfd	223
show bfd	224
show bfd interface	227
show hsc	229
BGP commands	231
address-family	231
aggregate-address	232
bgp add-paths select best 2	233
bgp always-compare-med	234
bgp asnotation dotted	235
bgp asnotation dotted-plus	236
bgp bestpath as-path ignore	236

bgp bestpath as-path multipath-relax	237
bgp bestpath compare-routerid	238
bgp bestpath med confed	239
bgp bestpath bgp-std-selection	240
bgp bestpath med missing-as-worst	241
bgp cluster id	241
bgp confederation	242
bgp confederation peers	243
bgp dampening	244
bgp default local-preference	245
bgp deterministic-med	246
bgp fast-external-fallover	247
bgp graceful-restart restart-time	248
bgp graceful-restart stalepath-time	248
bgp log-neighbor-changes	249
bgp maxas-limit	250
bgp router-id	251
bgp update-group	252
clear bgp	253
disable enable	255
distance bgp	255
maximum-paths	256
neighbor activate	258
neighbor advertisement-interval	259
neighbor add-paths	260
neighbor add-paths advertise-best	261
neighbor allowas-in	263
neighbor ao	264
neighbor capability orf prefix-list	266
neighbor default-originate	267
neighbor ebgp-multihop	268
neighbor fall-over	269
neighbor fall-over bfd	270
neighbor graceful-shutdown	272
neighbor interface	274
neighbor listen ip-range	275
neighbor local-as	277
neighbor maximum-prefix	279
neighbor next-hop-self	281
neighbor next-hop-unchanged	282
neighbor orf prefix-list in	283
neighbor passive	284
neighbor password	285
neighbor port	287
neighbor remote-as	288
neighbor remote as	289
neighbor remove-private-AS	291
neighbor replace-rt-asn	292
neighbor route-map	294
neighbor route-reflector-client	295
neighbor send-community	296
neighbor shutdown	298
neighbor slow-peer	300
neighbor soft-reconfiguration inbound	301
neighbor timers	302
neighbor timers connect-retry	303

neighbor ttl-security-hops	304
neighbor update-source	305
neighbor weight	306
network	307
redistribute	308
router bgp	310
show bgp	311
show bgp	314
show bgp community	316
show bgp flap-statistics	320
show bgp neighbor advertised-routes	321
show bgp neighbor paths	323
show bgp neighbor received orf-prefix-list	324
show bgp neighbor received-routes	326
show bgp neighbor routes	327
show bgp neighbors	329
show bgp paths	334
show bgp peer-group summary	335
show bgp summary	337
show bgp l2vpn evpn	339
show bgp l2vpn evpn vni route-type	342
show bgp l2vpn evpn vtep	343
show bgp l2vpn evpn vtep route-type	345
show bgp l2vpn evpn vtep vni	346
show bgp l2vpn evpn vtep vni route-type	347
show bgp ip unicast	348
show ip ospf routes	350
show running-config bgp	354
timers bgp	354
vrf	355
BIDIR-PIM commands	356
ip pim-bidir	356
ip pim-bidir hello-delay	357
ip pim-bidir lan-prune-delay	358
ip pim-bidir override-interval	359
ip pim-bidir propagation-delay	360
no ip pim-bidir	361
show ip pim dfe	362
show ip pim dfe	363
show running-config pim	364
BIDIR-PIM6 commands for IPv6	365
ipv6 pim6-bidir	365
ipv6 pim6-bidir hello-interval	366
ipv6 pim6-bidir hello-delay	367
ipv6 pim6-bidir lan-prune-delay	367
ipv6 pim6-bidir override-interval	368
ipv6 pim6-bidir propagation-delay	369
show ipv6 pim6 dfe	370
Boot commands	372
boot set-default	372
boot system	372
show boot-history	374

Breakout cable support commands	377
split	377
CDP commands	380
cdp	380
clear cdp counters	381
clear cdp neighbor-info	381
show cdp	382
show cdp neighbor-info	383
show cdp traffic	384
show cdp voice-vlan mode	385
Checkpoint commands	386
checkpoint auto	386
checkpoint auto confirm	387
checkpoint diff	388
checkpoint post-configuration	391
checkpoint post-configuration timeout	392
checkpoint rename	393
checkpoint rollback	393
copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL>	394
copy checkpoint <CHECKPOINT-NAME> {running-config startup-config}	396
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>	396
copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME>	397
copy <REMOTE-URL> startup-config running-config	398
copy running-config {startup-config checkpoint <CHECKPOINT-NAME>}	400
copy {running-config startup-config} <REMOTE-URL>	401
copy {running-config startup-config} <STORAGE-URL>	403
copy startup-config running-config	404
copy <STORAGE-URL> running-config	405
erase	406
show checkpoint <CHECKPOINT-NAME>	407
show checkpoint <CHECKPOINT-NAME> hash	410
show checkpoint post-configuration	411
show checkpoint	411
show checkpoint date	412
show running-config hash	413
show startup-config hash	414
write memory	415
Classifier policy commands	416
Classifier policy application	416
apply policy (config-if, config-lag-if, config-if-vlan, config-vlan)	416
apply policy	420
class copy	421
class ip	423
class ipv6	430
class mac	436
class resequence	440
class reset	442
clear policy hitcounts	443
policy	445
policy copy	449
policy resequence	450
policy reset	451

show class	451
show policy	453
CLI session commands	459
alias	459
auto-confirm	460
configure terminal	461
disable	462
do	462
enable (manager context)	463
end	464
exit	464
list	465
logout	465
page	467
Pipe () command	468
repeat	469
session-timeout	470
show session-timeout	470
show alias	471
show history	472
CLI user session management commands	475
cli-session	475
Clock commands	478
clock date	478
clock datetime	478
clock time	479
clock timezone	480
show clock	480
Container management commands	482
container	482
container exec	483
enable	483
env	484
image-location	485
mount	487
network vrf	488
port-map	489
restrict cpu	491
restrict memory	492
show container	492
show capacities containers	495
show capacities-status containers	495
show running-config container	496
vrf	497
CoPP commands	498
Classes of traffic	498
apply copp-policy	500
class	501
clear copp-policy statistics	502
copp-policy	504
default-class	505

reset copp-policy	506
show copp-policy	507
show copp-policy factory-default	509
show copp-policy statistics	510
show tech copp	512
Debug logging commands	514
clear debug buffer	514
debug {all <MODULE-NAME>}	515
debug db	516
debug destination	518
diag event-trap-disable	520
show debug	521
show debug buffer	522
show debug destination	523
DHCP client commands	525
ip dhcp	525
ipv6 dhcp	526
ip dhcp option	528
ip dhcp preferred-vlan	529
show ip dhcp	530
show ipv6 dhcp	531
show ip dhcp preferred-vlan	532
DHCPv4 relay commands	534
dhcp-relay	534
dhcp-relay hop-count-increment	534
dhcp-relay l2vpn-clients	535
dhcp-relay option 82	536
dhcp-relay vsx active-active	538
dhcp-smart-relay	538
diag-dump dhcp-relay basic	539
ip bootp-gateway	541
ip helper-address	542
show dhcp-relay	543
show dhcp-relay bootp-gateway	544
show ip helper-address	545
DHCP relay (IPv6) commands	547
dhcpv6-relay	547
dhcpv6-relay option 79	548
dhcpv6-relay vsx active-active	549
diag-dump dhcpv6-relay basic	549
ipv6 helper-address	551
show dhcpv6-relay	552
show ipv6 helper-address	553
DHCP server IPv4 commands	555
authoritative	555
bootp	555
clear dhcp-server leases	557
default-router	558
dhcp-server external-storage	559
dhcp-server vrf	560
disable	561

dns-server	561
domain-name	562
enable	563
lease	564
netbios-name-server	565
netbios-node-type	566
option	566
pool	568
range	569
show dhcp-server	570
static-bind	572
DHCP server IPv6 commands	574
authoritative	574
clear dhcpv6-server leases	575
dhcpv6-server external-storage	576
dhcpv6-server vrf	577
disable	578
dns-server	578
enable	579
lease	580
option	581
pool	582
range	583
show dhcpv6-server	584
static-bind	586
DHCP options commands	588
http-proxy	588
DNS client commands	590
ip dns domain-list	590
ip dns domain-name	591
ip dns host	592
ip dns server address	593
ip dns fqdn-resolver refresh-interval	594
ip dns fqdn-resolver force-refresh	595
show ip dns	596
show ip dns fqdn-resolver	598
show ip dns fqdn-resolver detail	599
show ip dns fqdn-resolver refresh-interval	601
ECMP commands	603
ip ecmp dynamic-mode	603
show ip ecmp	604
ERPS Commands	607
clear erps ring <RINGID> instance <ID>	607
clear erps statistics	607
erps ring	608
erps ring <RINGID> <port0 port1> interface	609
erps ring <RINGID> description	610
erps ring <RINGID> guard-interval	611
erps ring <RINGID> hold-off-interval	612
erps ring <RINGID> instance	613
erps ring <RINGID> instance <ID> control-vlan	614

erps ring <RINGID> instance <ID> description	615
erps ring <RINGID> instance <ID> enable	616
erps ring <RINGID> instance <ID> protected-vlans	617
erps ring <RINGID> instance <ID> protection-switch {manual force} <PORT0> <PORT1> ..	618
erps ring <RINGID> instance <ID> revertive	620
erps ring <RINGID> instance <ID> role	621
erps ring <RINGID> instance <ID> rpl	622
erps ring <RINGID> meg-level	623
erps ring <RINGID> parent-ring	624
erps ring <RINGID> sub-ring	625
erps ring <RINGID> tcn-propagation	626
erps ring <RINGID> transmission-interval	627
erps ring <RINGID> wtr-interval	628
show erps statistics	629
show erps status	630
show erps summary	633

EVPN commands 634

active-gateway	634
arp-suppression	636
arp-suppression {enable disable}	637
arp-suppression {enable disable}	638
arp-suppression exclude	640
dyn-vxlan-tunnel-bridging-mode	641
disable (evpn vlan-aware-bundles)	642
enable (evpn vlan-aware-bundles)	643
evpn	643
igmp-mld-proxy	644
igmp-mld-proxy forward-to-non-proxy	645
mac-move-detection count timer	646
nd-suppression	647
nd-suppression (enable disable)	648
nd-suppression exclude (per VLAN)	650
rd	651
rd (evpn vlan-aware-bundles)	652
redistribute host-route	653
redistribute host-route (evpn vlan-aware-bundles)	653
redistribute local-mac	654
redistribute local-svi	655
route-target	656
route-target auto mode	657
route-target {evpn}	658
route-target (evpn vlan-aware-bundles)	659
show evpn evi	660
show evpn evi summary	661
show evpn evi <EVI-ID>	662
show evpn evi detail	663
show evpn evi <EVI-ID> detail	665
show evpn evi igmp snooping	666
show evpn mac-ip	667
show evpn mac-ip evi	668
show evpn evi mld snooping	669
show evpn vtep-neighbor	670
show running-config evpn	671
virtual-mac	673
vlan	673

vlan-aware-bundle	674
vlan-ethernet-tag (evpn vlan-aware-bundles)	675
vlan <ID-RANGE>	676
External storage commands	678
address	678
directory	679
disable	680
enable	680
external-storage	681
password (external-storage)	682
show external-storage	683
show running-config external-storage	684
type	684
username	685
vrf	686
Feature pack commands	688
erase feature-pack	688
feature-pack mode	689
feature-pack server	690
feature-pack validate	692
show feature-pack	692
fast-reroute	697
neighbor	698
show capacities fast-reroute	699
show capacities status fast-reroute	700
Fault monitor commands	701
(Fault enabling/disabling)	701
action	702
apply fault-monitor profile	705
fault-monitor profile	706
show fault-monitor profile	707
show interface fault-monitor profile	708
show interface fault-monitor status	709
show running-config	710
threshold	712
vsx-sync (fault monitor)	714
Firmware management commands	716
copy {primary secondary} <REMOTE-URL>	716
copy {primary secondary} <FIRMWARE-FILENAME>	717
copy primary secondary	718
copy <REMOTE-URL>	718
copy secondary primary	720
copy <STORAGE-URL>	721
copy hot-patch	722
hot-patch	723
show hot-patch	725
Flow monitoring commands	726
diag-dump ipfix basic	726
description	727
exporter	728
flow exporter	730

flow monitor	733
flow record	735
ip flow monitor (interface)	737
show flow monitor	738
show flow record	741
show tech ipfix	743
gNMI commands	744
crypto pki application gnmi certificate	744
gnmi vrf	745
show gnmi	746
Hibernation commands	747
hibernate now	747
hibernate periodic	748
show hibernation	750
show running-config (hibernation)	751
High Availability Commands	752
redundancy switchover	752
HSC commands	754
bfd enable	754
bfd disable	754
disable	755
enable	756
hsc	756
manager ip	757
manager port	758
HTTPS server commands	760
https-server authentication certificate	760
https-server authentication password	761
https-server max-user-sessions	761
https-server rest access-mode	762
https-server rest firmware-site-distribution	763
https-server session close all	764
https-server session-timeout	765
https-server vrf	766
show https-server	767
show https-server authentication	769
show https-serverrest images	769
ICMP commands	771
ip icmp redirect	771
ip icmp throttle	771
ip icmp unreachable	772
IGMP commands	774
ip igmp	774
ip igmp apply access-list	775
ip igmp last-member-query-interval	777
ip igmp querier	778
ip igmp querier interval	779
ip igmp querier-wait-time	780

ip igmp querier query-max-response-time	781
ip igmp robustness	782
ip igmp router-alert-check	783
ip igmp static-group	784
ip igmp version	785
ip igmp version strict	786
no ip igmp	787
show ip igmp	788
show ip igmp counters	791
show ip igmp group	792
show ip igmp groups	795
show ip igmp interface	798
show ip igmp interface counters	800
show ip igmp interface group	801
show ip igmp interface groups	804
show ip igmp interface statistics	806
show ip igmp static-groups	807
show ip igmp statistics	809

Inband Flow Analyzer (IFA) commands 811

class	811
class ipv4/ipv6 filter	812
flow-filter-class	813
flow ifa-initiator-monitor	814
flow-telemetry-profile	815
ifa-device-id	816
ifa-hop-limit	817
ifa-max-metadata-stack-length	818
ifa-sampling-rate	819
ip-all flow ifa-terminator-monitor	819
ip-all flow ifa-transit-monitor	820
{ip ipv6} flow ifa-initiator-monitor	821
show flow ifa metrics	823
show flow ifa monitor-status all	827
show running-config	828

IGMP snooping commands 831

ip igmp snooping all-vlans	831
ip igmp snooping apply access list	831
ip igmp snooping querier-address	833
ip igmp snooping static group	834
ip igmp snooping (config mode)	835
ip igmp snooping (interface mode)	836
ip igmp snooping (vlan mode)	838
show ip igmp snooping	840

In-System Programming commands 844

clear update-log	844
show needed-updates	844

Interface commands 846

allow-unsupported-transceiver	846
default interface	848
description	849
error-control	849
flow-control	850

flow-control buffer headroom	855
flow-control buffer xon	856
flow-control buffer xoff dynamic	857
flow-control buffer xoff static	858
flow-control watchdog	860
flow-control watchdog timeout resume	861
interface	862
interface loopback	863
interface vlan	863
ip address	864
ip mtu	866
ip source-interface	867
ip tcp mss	868
ip unnumbered	869
ipv6 address	871
ipv6 source-interface	873
ipv6 tcp mss	874
l3-counters	875
mtu	876
persona	877
rate-interval	880
routing	881
show allow-unsupported-transceiver	882
show interface	883
show interface dom	889
show interface flow-control	890
show interface link-diagnostics	895
show interface profile	898
show interface statistics	899
show interface transceiver	902
show interface supported-transceivers	906
show interface utilization	910
show ip interface	911
show ip source-interface	912
show ipv6 interface	913
show ipv6 source-interface	915
show system interface-group	916
show system interface-profile	918
shutdown	918
system interface-group	919
system interface-profile	921
IP Directed Broadcast commands	924
copy support-file feature	924
ip directed-broadcast	924
show arp	925
show ip interface	926
show ip directed-broadcast	927
IP Neighbor Flood commands	929
ip neighbor-flood	929
show ip interface	929
show ip neighbor-flood	930
show running-config	931
IP-SLA commands	932

http	932
https	934
icmp-echo	936
ip-sla	937
ip-sla responder	938
show ip-sla all	940
show ip-sla responder	942
show ip-sla	943
start-test	945
stop-test	946
tcp-connect	946
udp-echo	948
udp-jitter-voip	949
vrf	951

IP tunnels commands 953

description	953
destination ip	954
destination ipv6	955
interface tunnel	956
ip address	958
ipv6 address	959
ip mtu	960
show interface tunnel	961
show running-config interface tunnel	963
shutdown	965
source ip	966
source ipv6	967
ttl	968
vrf attach	969

IPv6 RA commands 971

ip dhcp option ipv6-only-preferred	971
ipv6 address <global-unicast-address>	973
ipv6 address autoconfig	973
ipv6 address link-local	974
ipv6 nd cache-limit	975
ipv6 nd dad attempts	976
ipv6 nd hop-limit	977
ipv6 nd mtu	978
ipv6 nd ns-interval	978
ipv6 nd prefix	979
ipv6 nd ra dns search-list	981
ipv6 nd ra dns server	981
ipv6 nd ra lifetime	982
ipv6 nd ra managed-config-flag	983
ipv6 nd ra max-interval	984
ipv6 nd ra min-interval	985
ipv6 nd ra other-config-flag	986
ipv6 nd ra reachable-time	987
ipv6 nd ra retrans-timer	988
ipv6 nd route	988
ipv6 nd router-preference	990
ipv6 nd suppress-ra	990
show ipv6 nd global traffic	991
show ipv6 nd interface	992

show ipv6 nd interface prefix	997
show ipv6 nd interface route	998
show ipv6 nd ra dns search-list	999
show ipv6 nd ra dns server	1000
IRDP commands	1002
diag-dump irdp basic	1002
ip irdp	1003
ip irdp holdtime	1004
ip irdp maxadvertinterval	1005
ip irdp minadvertinterval	1006
ip irdp preference	1007
show ip irdp	1008
IVRF commands	1010
address-family	1010
ip ipv6 vrf	1011
ipv6 route source interface	1014
ip route interface	1016
rd	1019
redistribute	1020
route-target	1021
route-target export	1023
router bgp	1024
router bgp vrf	1025
show bgp vpn unicast	1026
show bgp info vrf	1030
show ip route vrf	1031
show ipv6 route vrf	1032
vrf	1034
Job Scheduler commands	1036
job	1036
reload	1038
schedule	1040
show job	1043
show capacities (job, schedule)	1045
show reload	1046
show running-config (job, schedule)	1047
show schedule	1048
Key chain commands	1051
accept-lifetime	1051
cryptographic-algorithm	1052
key	1053
keychain	1054
key-string	1055
name	1056
recv-id	1057
send-lifetime	1058
send-id	1059
show capacities keychain	1060
show keychain	1061
show running-config keychain	1063
show interface	1063

LACP and LAG commands	1071
description	1071
interface lag	1072
interface persona lag	1073
ip address	1074
ipv6 address	1075
lacp fallback	1076
lacp fallback-static	1077
lacp hash	1078
lacp mode	1078
lacp port-id	1079
lacp port-priority	1080
lacp rate	1081
lacp system-priority	1082
lag	1083
persona custom	1084
show interface	1086
show interface persona	1087
show lacp aggregates	1088
show lacp configuration	1089
show lacp interfaces	1090
show lag	1094
show running-config interface	1095
shutdown	1098
vlan trunk native	1099
 LLDP commands	 1101
clear lldp neighbors	1101
clear lldp statistics	1101
lldp	1102
lldp dot3	1103
lldp dot3 mfs	1104
lldp management-address vlan	1104
lldp management-ip-address	1105
lldp management-ipv6-address	1106
lldp med	1107
lldp med location	1109
lldp receive	1111
lldp reinit	1112
lldp select-tlv	1112
lldp timer	1114
lldp tlv-enable	1115
lldp transmit	1116
lldp txdelay	1117
lldp trap enable	1118
show lldp configuration	1120
show lldp configuration mgmt	1122
show lldp local-device	1123
show lldp neighbor-info	1125
show lldp neighbor-info detail	1128
show lldp neighbor-info mgmt	1131
show lldp statistics	1132
show lldp statistics mgmt	1134
show lldp tlv	1135
 Local AAA commands	 1136

aaa accounting all-mgmt	1136
aaa authentication console-login-attempts	1138
aaa authentication limit-login-attempts	1139
aaa authentication login	1140
aaa authentication login privilege-elevation	1141
aaa authentication minimum-password-length	1142
aaa authorization commands (local)	1143
show aaa accounting	1145
show aaa authentication	1146
show aaa authorization	1147
show authentication locked-out-users	1148
show ssh authentication-method	1149
show user	1150
ssh password-authentication	1151
ssh public-key-authentication	1152
user authorized-key	1152
Log rotation commands	1155
logging threshold	1155
logrotate maxsize	1157
logrotate period	1157
logrotate target	1158
show logrotate	1160
Loop protect commands	1161
loop-protect	1161
loop-protect action	1162
loop-protect re-enable-timer	1163
loop-protect transmit-interval	1164
loop-protect trap loop-detected	1164
loop-protect vlan	1165
show loop-protect	1166
Loopback commands	1170
interface loopback	1170
ip address	1170
ipv6 address	1171
vrf attach	1172
show interface loopback	1173
MAC address table commands	1175
clear mac-address	1175
clear mac address mac move	1177
clear mac-address-table	1178
mac-address-table age-time	1178
show mac-address-table	1179
show mac-address-table address	1181
show mac-address-table count	1181
show mac-address-table dynamic	1183
show mac-address-table interface	1184
show mac-address-table lockout	1185
show mac address table mac move	1186
show mac-address-table mac-move	1187
show mac-address-table port	1189
show mac-address-table static	1190
show mac-address-table vlan	1190

show mac address table mac move	1191
static-mac	1192
MACsec commands	1194
apply macsec policy	1194
bypass	1195
cipher-suite (MACsec)	1197
clear macsec statistics	1198
clear tag mode	1199
confidentiality	1200
include-sci-tag	1201
macsec policy	1202
macsec selftest	1203
replay-protection	1203
show macsec policy	1204
show macsec selftest	1205
show macsec statistics	1207
show macsec status	1209
Management interface commands	1212
default-gateway	1212
ip static	1213
nameserver	1214
show interface mgmt	1215
mDNS gateway commands	1216
debug mdns	1216
description	1217
id	1217
mdns-sd	1218
mdns-sd apply-profile tx	1219
mdns-sd enable	1220
mdns-sd profile	1221
mdns-sd service	1221
clear mdns-sd statistics	1222
sequence-number	1223
show mdns-sd service-entries	1224
show mdns-sd statistics	1226
show mdns-sd statistics profile	1226
show mdns-sd summary	1227
show running-config interface	1228
show running-config mdns-sd profile	1229
show running-config mdns-sd service	1230
Mirroring commands	1231
clear mirror	1231
comment	1231
copy tcpdump-pcap	1232
copy tshark-pcap	1233
destination cpu	1234
destination interface	1235
destination tunnel	1236
diagnostic	1238
diag utilities tcpdump	1239
disable	1241
enable	1242

mirror session	1243
show mirror	1244
source interface	1246
MKA commands (MACsec)	1249
apply mka policy	1249
clear mka statistics	1250
data-delay-protection	1251
eapol-destination-mac	1252
eapol-dot1q-tagged	1253
eapol-eth-type	1254
key-server-priority	1256
pre-shared-key	1257
mka policy	1258
show mka policy	1259
show mka statistics	1260
show mka status	1261
transmit-interval	1263
MLD snooping global configuration commands	1264
ipv6 mld snooping	1264
MLD snooping VLAN configuration commands	1265
ipv6 mld snooping	1265
ipv6 mld snooping apply access-list	1266
ipv6 mld snooping all-vlans	1267
ipv6 mld snooping auto vlan	1268
ipv6 mld snooping blocked vlan	1269
ipv6 mld snooping fastlearn	1270
ipv6 mld snooping fastleave vlan	1271
ipv6 mld snooping forced fastleave vlan	1272
ipv6 mld snooping forward vlan	1273
ipv6 mld snooping querier-address	1274
ipv6 mld snooping static-group	1275
ipv6 mld snooping version	1276
MLD snooping show commands	1278
show ipv6 mld snooping	1278
show mgmd debug-counters	1281
MLD configuration commands for interface VLAN	1283
ipv6 mld	1283
ipv6 mld apply access-list	1283
no ipv6 mld	1285
ipv6 mld querier	1285
ipv6 mld querier interval	1286
ipv6 mld querier-wait-time	1287
ipv6 mld last-member-query-interval	1288
ipv6 mld querier query-max-response-time	1288
ipv6 mld robustness	1289
ipv6 mld static-group	1290
ipv6 mld version	1291
ipv6 mld version strict	1292
MLD show commands for interface VLAN	1293

show ipv6 mld	1293
MLD configuration commands for interface	1298
ipv6 mld	1298
ipv6 mld apply access-list	1298
no ipv6 mld	1300
ipv6 mld querier	1300
ipv6 mld querier interval	1301
ipv6 mld last-member-query-interval	1302
ipv6 mld querier query-max-response-time	1303
ipv6 mld robustness	1303
ipv6 mld static-group	1304
ipv6 mld version	1305
ipv6 mld version strict	1306
MSDP router config commands	1307
disable	1307
enable	1307
router msdp	1308
sa-interval	1309
sa-limit	1309
MSDP peer configuration commands	1312
connection-retry-interval	1312
connect-source	1312
clear ip msdp peer statistics	1313
description	1314
disable	1315
enable (ip msdp peer)	1316
ip msdp peer	1316
keepalive	1317
mesh-group	1318
password (router msdp)	1319
sa-filter access-list	1320
MSDP show commands	1322
show ip msdp count	1322
show ip msdp peer	1323
show ip msdp sa-cache	1324
show ip msdp summary	1325
MSTP commands	1327
clear spanning-tree statistics	1327
show spanning-tree	1327
show spanning-tree detail	1329
show spanning-tree inconsistent-ports	1331
show spanning-tree mst	1332
show spanning-tree mst-config	1334
show spanning-tree mst detail	1335
show spanning-tree mst <INSTANCE-ID>	1338
show spanning-tree mst <INSTANCE-ID> detail	1340
show spanning-tree mst interface	1341
show spanning-tree summary port	1342
show spanning-tree summary root	1343
spanning-tree	1344
spanning-tree bpdu-filter	1345

spanning-tree bpduguard	1346
spanning-tree bpduguard timeout	1347
spanning-tree config-name	1348
spanning-tree config-revision	1349
spanning-tree cost	1350
spanning-tree forward-delay	1351
spanning-tree hello-time	1352
spanning-tree instance cost	1353
spanning-tree instance port-priority	1354
spanning-tree instance priority	1355
spanning-tree instance vlan	1356
spanning-tree link-type	1357
spanning-tree loop-guard	1357
spanning-tree max-age	1358
spanning-tree max-hops	1359
spanning-tree mode	1360
spanning-tree port-priority	1362
spanning-tree port-type	1363
spanning-tree priority	1364
spanning-tree root-guard	1365
spanning-tree rpvst-filter	1366
spanning-tree rpvst-guard	1367
spanning-tree tcnguard	1368
spanning-tree transmit-hold-count	1369
spanning-tree trap	1369
Multicast VXLAN commands	1372
clear ip mroute	1372
ip pim-sparse datapath-auto-include	1373
ip pim-sparse vsx-virtual-neighbor	1374
datapath-auto-include	1375
ipv6 pim6-sparse vsx-virtual-neighbor	1376
register-source	1377
show ip mroute	1378
show ip pim neighbor	1381
show ipv6 mroute	1383
show ipv6 pim6 interface vlan	1385
show ipv6 pim6 neighbor	1386
ip multicast multi-fabric identifier	1389
Multicast datapath commands for IPv4	1391
show ip multicast bridging datapath	1391
show ip multicast routing datapath	1392
Multicast datapath commands for IPv6	1395
show ipv6 multicast bridging datapath	1395
show ipv6 multicast routing datapath	1396
Static Route commands	1399
ip multicast-static-route	1399
ip multicast-static-route (l3vni)	1401
ipv6 multicast-static-route	1402
ipv6 multicast-static-route (l3vni)	1404
redistribute static	1405
show capacities multicast static route	1406
show ip multicast-static-route	1407

show ip multicast-static-route detail	1408
show ip multicast-static-route (group)	1409
show ipv6 multicast-static-route	1412
show ipv6 multicast-static-route (group)	1414
show ipv6 multicast-static-route detail	1415
show running-config	1416
MVRP commands	1418
clear mvrp statistics	1418
mvrp	1418
mvrp registration	1419
mvrp timer	1420
show mvrp config	1421
show mvrp state	1422
show mvrp statistics	1423
ND snooping commands	1426
clear nd-snooping statistics	1426
nd-snooping	1426
nd-snooping (in config-vlan context)	1427
nd-snooping mac-check	1428
nd-snooping ra-guard	1429
nd-snooping trust	1430
show nd-snooping	1430
show nd-snooping statistics	1432
Network Analytics Engine commands	1434
nae cli-authorization	1434
show nae-agent	1434
show nae-agent alerts	1437
show nae-agent alerts details	1438
show nae-script	1440
uerieshow running-config (nae-lite)	1441
Network Analytics Engine Lite commands	1443
actions	1443
desc	1448
disable	1449
monitor resource	1449
nae-agent lite	1452
nae-agent lite activate	1453
2set-condition monitor	1454
5set-condition watch	1455
show running-config nae-agent	1457
tags	1458
watch event-log	1459
Network configuration validation commands	1461
switch config-validator	1461
NLB commands	1463
arp ip mac	1463
show arp	1464
show ip igmp snooping vlan group	1464

NTP commands	1467
ntp authentication	1467
ntp authentication-key	1467
ntp disable	1469
ntp enable	1469
ntp conductor	1470
ntp server	1471
ntp trusted-key	1473
ntp vrf	1474
show ntp associations	1475
show ntp authentication-keys	1476
show ntp servers	1477
show ntp statistics	1478
show ntp status	1479
 OSPFv2 commands	 1481
active-backbone	1481
area (ospf)	1481
area default-metric	1482
area nssa	1483
area range	1484
area stub	1486
area virtual-link	1487
authentication	1488
authentication-key	1489
clear ip ospf neighbors	1490
clear ip ospf statistics	1492
dead-interval	1493
default-information originate	1493
default-information originate always	1495
default-metric	1496
disable	1496
distance	1497
distribute-list prefix	1499
enable	1500
graceful-restart	1500
hello-interval	1502
ip ospf area	1503
ip ospf authentication	1504
ip ospf authentication-key	1505
ip ospf cost	1506
ip ospf dead-interval	1507
ip ospf hello-interval	1508
ip ospf keychain	1509
ip ospf message-digest-key md5	1510
ip ospf network	1511
ip ospf passive	1512
ip ospf priority	1513
ip ospf retransmit-interval	1514
ip ospf sha-key sha	1515
ip ospf shutdown	1516
ip ospf transit-delay	1517
keychain	1518
max-metric router-lsa	1518
maximum-paths	1519
message-digest-key md5	1520

passive-interface default	1522
redistribute	1522
reference-bandwidth	1524
retransmit-interval	1525
rfc1583-compatibility	1526
router ospf	1527
router-id	1528
sha-key sha	1529
show ip ospf	1530
show ip ospf border-routers	1531
show ip ospf interface	1532
show ip ospf lsdb	1535
show ip ospf neighbors	1540
show ip ospf routes	1542
show ip ospf statistics	1546
show ip ospf statistics interface	1547
show ip ospf virtual-links	1548
summary-address	1550
timers lsa-arrival	1551
timers throttle lsa	1552
timers throttle spf	1553
transit-delay	1554
trap-enable	1555

OSPFv3 commands 1557

active-backbone	1557
area	1557
area authentication ipsec	1558
area encryption ipsec	1560
area nssa	1562
area range	1563
area stub	1564
area virtual-link	1565
area default-metric	1566
authentication ipsec	1567
clear ipv6 ospfv3 neighbors	1569
clear ipv6 ospfv3 statistics	1570
dead-interval	1571
default-information originate	1572
default-metric	1573
disable	1573
distance	1574
distribute-list prefix	1576
enable	1577
encryption ipsec	1577
default-information originate	1579
default-information originate always	1580
graceful-restart	1582
hello-interval	1583
ipv6 ospfv3 area	1584
ipv6 ospfv3 authentication null	1585
ipv6 ospfv3 authentication ipsec	1586
ipv6 ospfv3 cost	1587
ipv6 ospfv3 dead-interval	1588
ipv6 ospfv3 encryption ipsec	1589
ipv6 ospfv3 encryption null	1591

ipv6 ospfv3 hello-interval	1591
ipv6 ospfv3 network	1592
ipv6 ospfv3 passive	1593
ipv6 ospfv3 priority	1594
ipv6 ospfv3-af retransmit-interval	1595
ipv6 ospfv3 shutdown	1596
ipv6 ospfv3 transit-delay	1596
maximum-paths	1597
max-metric router-lsa	1598
passive-interface default	1599
redistribute	1600
reference-bandwidth	1602
retransmit-interval	1603
router-id	1604
router ospfv3	1605
show ipv6 ospfv3	1606
show ipv6 ospfv3 border-routers	1607
show ipv6 ospfv3 interface	1608
show ipv6 ospfv3 lsdb	1611
show ipv6 ospfv3 neighbors	1615
show ipv6 ospfv3 routes	1617
show ipv6 ospfv3 statistics	1619
show ipv6 ospfv3 statistics interface	1620
show ipv6 ospfv3 virtual-links	1622
summary-address	1623
timers lsa-arrival	1624
timers throttle lsa	1625
timers throttle spf	1626
transit-delay	1628
trap-enable	1629

OSPFv3 AF commands 1629

active-backbone stub-default-rout	1629
address-family unicast	1630
area default-metric	1631
area nssa	1632
area	1633
area range	1635
area stub	1636
area virtual-link	1638
authentication ipsec spi	1639
clear ospfv3-af ipv4 neighbor	1640
clear ospfv3-af ipv4 statistics	1642
clear ospfv3-af ipv6 neighbor	1643
clear ospfv3-af ipv6 statistics	1644
dead-interval	1645
debug ospfv3-af	1646
default-information originate always	1648
default-information originate	1649
default-metric	1650
diag ospfv3 lsdb dump	1650
disable	1652
distance	1653
distribute-list prefix	1654
enable	1656
encryption ipsec	1656

graceful-restart ignore-lost-interface	1659
graceful-restart	1660
hello-interval	1661
ospfv3-af ipv4 retransmit-interval	1662
ospfv3-af ipv4 cost	1663
ospfv3-af ipv4 hello-interval	1664
ospfv3-af ipv4 network	1665
ospfv3-af ipv4 priority	1666
ospfv3-af ipv4 shutdown	1666
ospfv3-af ipv4 transit-delay	1667
ospfv3-af ipv6 area	1668
ospfv3-af ipv6 cost	1669
ospfv3-af ipv6 dead-interval	1670
ospfv3-af ipv6 hello-interval	1671
ospfv3-af ipv6 network	1672
ospfv3-af ipv6 passive	1673
ospfv3-af ipv6 priority	1674
ospfv3-af ipv6 retransmit-interval	1675
ospfv3-af ipv6 shutdown	1675
ospfv3-af ipv6 transit-delay	1676
max-metric router-lsa	1677
maximum-paths	1679
OSPFv3 AF commands	1680
ospfv3-af encryption ipsec spi	1680
ospfv3-af authentication ipsec spi	1681
ospfv3-af encryption ipsec	1683
ospfv3-af ipv4 area	1685
ospfv3-af ipv4 dead-interval	1686
ospfv3-af authentication null	1687
ospfv3-af encryption null	1688
ospfv3-af ipv4 passive	1688
passive-interface default	1689
redistribute	1690
reference-bandwidth	1692
retransmit-interval	1693
router-id	1694
router ospfv3-af	1696
show ospfv3-af ipv4 statistics	1697
show debug buffer module ospfv3-af	1698
show ospfv3-af ipv4	1701
show ospfv3-af ipv4 border-routers	1703
show ospfv3-af ipv4 interface	1704
show ospfv3-af ipv4 lsdb	1707
show ospfv3-af ipv4 neighbors	1713
show ospfv3-af ipv4 routes	1716
show ospfv3-af ipv4 statistics interface	1718
show ospfv3-af ipv6	1721
show ospfv3-af ipv6 border-routers	1723
show ospfv3-af ipv6 interface	1724
show ospfv3-af ipv6 lsdb	1727
show ospfv3-af ipv6 neighbors	1733
show ospfv3-af ipv6 routes	1736
show ospfv3-af ipv6 statistics	1738
show ospfv3-af ipv6 statistics interface	1739
show ospfv3-af ipv6 virtual-links	1742
show running-config	1744

show running-config all	1748
show tech ospfv3-af	1758
summary-address	1764
timers lsa-arrival	1765
timers throttle lsa	1766
timers throttle spf	1767
transit-delay	1769
packet-capture commands	1770
copy packet-capture	1770
packet-capture delete-pcap	1771
packet-capture enable	1771
packet-capture	1773
packet-capture commands	1775
show packet-capture pcaps	1775
show packet-capture session	1776
PBR commands	1778
apply policy	1778
pbr-action-list	1779
pbr-action-list copy	1782
pbr-action-list resequence	1783
pbr-action-list reset	1784
policy	1785
show pbr	1788
show pbr-action-list	1789
show running-config current-context	1791
Backup nexthop group commands	1792
ip nexthop group type backup	1792
primary secondary nexthop	1793
show ip nexthop group name type backup	1794
show ip nexthop group type backup	1795
PIM-DM commands for IPv4	1797
disable	1797
enable	1797
ip pim-dense	1798
ip pim-dense bfd	1799
ip pim-dense graft-retry-interval	1800
ip pim-dense hello-delay	1801
ip pim-dense hello-interval	1802
ip pim-dense ip-addr	1803
ip pim-dense lan-prune-delay	1804
ip pim-dense max-graft-retries	1804
ip pim-dense override-interval	1805
ip pim-dense propagation-delay	1806
ip pim-dense ttl-threshold	1807
router pim	1808
show ip mroute	1815
show ip mroute group-addr	1817
show ip mroute brief	1818
show ip pim	1819
show ip pim interface	1820
show ip pim interface interface-name	1822
show ip pim interface interface-name counters	1823

show ip pim rpf	1824
show ip pim neighbor	1826
state-refresh-interval	1827

PIM-DM commands for IPv6 **1829**

enable	1829
ipv6 pim6-dense	1830
ipv6 pim6-dense bfd	1831
ipv6 pim6-dense graft-retry-interval	1832
ipv6 pim6-dense hello-delay	1833
ipv6 pim6-dense hello-interval	1834
ipv6 pim6-dense ipv6-addr	1835
ipv6 pim6-dense lan-prune-delay	1836
ipv6 pim6-dense max-graft-retries	1837
ipv6 pim6-dense override-interval	1837
ipv6 pim6-dense propagation-delay	1838
ipv6 pim6-dense ttl-threshold	1839
no ipv6 pim6-dense	1840
register-source	1841
router pim6	1842
show ipv6 pim6	1843
show ipv6 pim6 interface	1844
show ipv6 pim6 interface <INTERFACE-NAME>	1845
show ipv6 pim6 rpf	1846
show ipv6 mroute	1848
show ipv6 mroute brief	1850
show ipv6 mroute <GROUP-ADDR>	1851
show ipv6 pim6 neighbor	1853
state-refresh-interval	1855

PIM-SM commands for IPv4 **1857**

accept-register access-list	1857
accept-rp	1858
active-active	1859
anycast-rp source-directly-connected	1860
bfd all-interfaces	1861
bsr-candidate bsm-interval	1862
bsr-candidate hash-mask-length	1862
bsr-candidate priority	1863
bsr-candidate source-ip-interface	1864
disable	1865
enable	1866
ip mroute	1866
ip multicast boundary	1868
ip multicast multipath	1869
ip ipv6 multicast rpf	1870
ip pim-sparse	1876
ip pim-sparse bfd	1876
ip pim-sparse bsr-boundary	1877
ip pim-sparse dr-priority	1878
ip pim-sparse hello-delay	1879
ip pim-sparse hello-interval	1880
ip pim-sparse ip-addr	1881
ip pim-sparse lan-prune-delay	1882
ip pim-sparse override-interval	1883
ip pim-sparse propagation-delay	1884

ipv6 multicast rpf	1885
join-prune-interval	1889
multicast-route-limit	1890
no ip pim-sparse	1891
register-rate-limit	1891
register-source	1892
router pim	1893
rp-address	1900
rp-address access list	1901
rp-candidate group-prefix	1902
rp-candidate hold-time	1903
rp-candidate priority	1904
rp-candidate source-ip-interface	1905
rpf-override	1906
show ip mroute	1907
show ip mroute brief	1909
show ip mroute group-addr	1910
show ip multicast anomalies	1911
show ip multicast boundary interface	1913
show ip pim	1913
show ip pim rpf	1915
show ip pim bsr	1916
show ip pim bsr elected	1918
show ip pim bsr local	1919
show ip pim interface	1920
show ip pim interface interface-name	1922
show ip pim interface interface-name counters	1924
show ip pim rp	1927
show ip pim rp-registered-source	1928
show ip pim neighbor	1930
show ip pim pending	1931
show ip pim rp-candidate	1932
show ip pim rp-set	1934
show ip pim rp-set learned	1935
show ip pim rp-set static	1936
show ip pim rpf-override	1937
show ip pim rp-registered-source	1938
show ip pim rpf-override source	1940
show ip pim tree-state	1941
sources-per-group	1944
spt-threshold	1945

PIM-SM commands for IPv6 1946

accept-register access-list	1946
accept-rp	1947
bsr-candidate bsm-interval	1948
bsr-candidate hash-mask-length	1949
bsr-candidate priority	1950
bsr-candidate source-ip-interface	1950
enable	1952
ipv6 mroute	1953
ipv6 pim6-sparse	1954
ipv6 pim6-sparse bfd	1955
ipv6 pim6-sparse dr-priority	1956
ipv6 pim6-sparse hello-delay	1957
ipv6 pim6-sparse hello-interval	1958

ipv6 pim6-sparse ipv6-addr	1959
ipv6 pim6-sparse lan-prune-delay	1960
ipv6 pim6-sparse override-interval	1961
ipv6 pim6-sparse propagation-delay	1963
join-prune-interval	1964
no ipv6 pim6-sparse	1964
rp-address access list	1965
rp-address	1966
rp-candidate group-prefix	1967
rp-candidate hold-time	1968
rp-candidate priority	1969
rp-candidate source-ip-interface	1970
rpf-override	1971
show ipv6 mroute <GROUP-ADDR>	1973
show ipv6 mroute	1974
show ipv6 mroute brief	1976
show ipv6 pim6	1977
show ipv6 pim6 bsr	1978
show ipv6 pim6 bsr local	1981
show ipv6 pim6 interface	1983
show ipv6 pim6 neighbor	1984
show ipv6 pim6 pending	1985
show ipv6 pim6 rp	1986
show ipv6 pim6 rpf	1988
show ipv6 pim6 rp-candidate	1989
show ipv6 pim6 rpf-override	1990
show ipv6 pim6 rp-registered-source	1991
.....	1992
show ipv6 pim6 rp registered sources	1992
show ipv6 pim6 rpf-override source	1993
show ipv6 pim6 rp-set	1994
show ipv6 pim6 rp-set learned	1996
show ipv6 pim6 rp-set static	1997
show ipv6 pim6 tree-state	1998
sources-per-group	2000
spt-threshold	2001

PIM-SSM commands 2003

ip igmp apply ssm-map access-list	2003
show ip igmp ssm-map	2004

PIM-SSM commands for IPv4 2006

pim-ssm	2006
pim-ssm range-access-list	2007
show ip mroute	2008
show ip multicast summary	2009
show ip pim interface interface-name counters	2011

PIM-SSM commands for IPv6 2015

ipv6 mld apply ssm-map access-list	2015
pim-ssm	2016
pim-ssm range-access-list	2017
show ip multicast summary	2018
show ipv6 pim interface counters	2020
show ipv6 mld ssm-map	2022
show ipv6 mroute	2023

Ping commands	2026
ping	2026
ping6	2032
PKI commands	2036
crypto pki application	2036
crypto pki certificate	2038
crypto pki ta-profile	2039
enroll self-signed	2040
enroll terminal	2041
ext-key-usage	2042
import (CA-signed leaf certificate)	2043
import (self-signed leaf certificate)	2045
key-type	2047
key-usage	2048
ocsp disable-nonce	2049
ocsp enforcement-level	2050
ocsp url	2051
ocsp vrf	2052
revocation-check ocsp	2053
show crypto pki application	2054
show crypto pki certificate	2055
show crypto pki ta-profile	2057
subject	2059
subject-alt-name	2060
ta-certificate	2061
PKI EST commands	2064
arbitrary-label	2064
arbitrary-label-enrollment	2065
arbitrary-label-reenrollment	2066
crypto pki est-profile	2067
enroll est-profile	2068
reenrollment-lead-time	2070
retry-count	2070
retry-interval	2071
show crypto pki est-profile	2072
url	2073
username	2074
vrf	2076
Port filtering commands	2078
PTP commands	2079
clear ptp statistics	2079
clock-domain	2079
clock-step	2080
enable	2082
ip source-interface	2082
mode	2084
priority1	2085
priority2	2086
ptp announce-interval	2087
ptp announce-timeout	2088
ptp clock-source-only	2089

ptp delay-req-interval	2090
ptp enable	2091
ptp lag-role	2092
ptp peer ip	2093
ptp profile	2094
ptp sync-interval	2096
ptp vlan	2097
show ptp clock	2098
show ptp foreign-clock-sources	2099
show ptp interface	2100
show ptp parent	2103
show ptp time-property	2104
show running-config ptp	2105
transport-protocol	2106

QoS commands 2108

apply qos	2108
apply qos threshold-profile	2110
clear queue-monitor interface	2111
dwrr queue	2113
flow-control buffer cable-length	2114
map queue	2115
name queue	2117
qos cos-map	2118
qos counters ecn	2119
qos counters rocev2	2120
qos dscp	2121
qos dscp-map	2122
qos pool	2124
qos queue-profile	2126
qos schedule-profile	2127
qos shape	2128
qos threshold-profile	2130
qos trust	2131
queue action	2132
queue-monitor	2134
queue-monitor polling-interval seconds	2135
rate-limit	2137
show interface queues	2139
show interface queue-monitor	2140
show interface queue-monitor status	2143
show interface qos	2146
show interface qos buffers	2147
show interface qos counters	2150
show qos cos-map	2151
show qos dscp-map	2152
show qos pool	2153
show qos queue-profile	2156
show qos schedule-profile	2157
show qos threshold-profile	2158
show qos trust	2160
show queue-monitor status	2161
strict queue	2162

Remote AAA (TACACS+, RADIUS) commands 2165

aaa accounting allow-fail-through	2165

aaa accounting all-mgmt	2165
aaa authentication allow-fail-through	2168
aaa authentication login	2169
aaa authorization allow-fail-through	2171
aaa authorization commands	2173
aaa group server	2176
radius-server auth-type	2177
radius-server host	2178
radius-server host secure ipsec	2182
radius-server host tls (RadSec)	2187
radius-server host tls port-access	2190
radius-server key	2191
radius-server retries	2192
radius-server service-type in-access-request	2193
radius-server timeout	2193
radius-server tls timeout (RadSec)	2194
radius-server tracking	2195
server	2197
show aaa accounting	2199
show aaa authentication	2201
show aaa authorization	2204
show aaa server-groups	2206
show accounting log	2208
show radius-server	2211
show radius-server secure ipsec	2216
show radius-server authentication statistics	2218
show radius-server authentication statistics host	2219
show tacacs-server	2220
show tacacs-server statistics	2223
show tech aaa	2224
tacacs-server auth-type	2230
tacacs-server host	2231
tacacs-server key	2233
tacacs-server timeout	2234
tacacs-server tracking	2235

Remote syslog commands **2238**

clear accounting-logs	2238
diag persistent-storage	2239
logging	2240
logging accounting-format-native	2243
logging filter	2244
logging facility	2247
logging persistent-storage	2248

RIPv2 (IPv4) commands **2251**

Configuration commands	2251
router rip	2251
Interface commands	2252
ip rip	2252
ip rip all-ip enable	2253
ip rip all-ip disable	2254
ip rip all-ip send disable	2254
ip rip all-ip receive disable	2255
Routing commands	2256
enable	2256

disable	2257
distance	2258
maximum-paths	2258
redistribute	2259
timers update	2260
RIPv2 clear commands	2261
clear ip rip statistics	2261
RIPv2 interface commands	2262
enable	2262
disable	2263
send disable	2264
receive disable	2265
RIPv2 show commands	2265
show capacities rip	2266
show capacities-status rip	2266
show ip rip	2267
show ip rip interface	2268
show ip rip neighbors	2269
show ip rip routes	2271
show ip rip statistics	2272
show ip rip statistics interface	2273
show running-config	2274
RIPng (IPv6) commands	2276
Configuration commands	2276
router ripng	2276
Interface commands	2277
ipv6 ripng	2277
Routing commands	2278
enable	2278
disable	2278
distance	2279
maximum-paths	2280
redistribute	2281
timers update	2282
RIPng clear commands	2283
clear ipv6 ripng statistics	2283
RIPng interface commands	2284
enable	2284
disable	2284
send disable	2285
receive disable	2286
RIPng show commands	2287
show capacities ripng	2287
show capacities-status ripng	2287
show ipv6 ripng	2288
show ipv6 ripng interface	2289
show ipv6 ripng neighbors	2290
show ipv6 ripng routes	2292
show ipv6 ripng statistics	2293
show ipv6 ripng statistics interface	2294
show running-config	2295
Route policy and route map commands	2297
General or filtering commands	2297
ip aspath-list	2297

ip community-list	2298
ip prefix-list	2299
ipv6 prefix-list	2300
route-map	2301
continue	2302
Match commands	2304
match aspath-list	2304
match community-list	2304
match interface	2305
match ip address prefix-list	2306
match ip next-hop	2307
match ip route-source	2308
match local-preference	2308
match metric	2309
match origin	2310
match route-type	2310
match source-protocol	2311
match tag	2312
match vni	2313
Set commands	2314
set as-path exclude	2314
set as-path prepend	2315
set community	2315
set dampening	2316
set ip nexthop	2317
set local-preference	2318
set metric	2319
set origin	2320
set tag	2320
set weight	2321
Show commands	2322
show ip aspath-list	2322
show ip community-list	2323
show ip prefix-list	2324
show route-map	2324

RPVST+ commands 2327

clear spanning-tree statistics	2327
show capacities-status rpvst	2327
show spanning-tree	2328
show spanning-tree detail	2329
show spanning-tree inconsistent-ports	2331
show spanning-tree summary port	2332
show spanning-tree summary root	2333
show spanning-tree vlan	2334
show spanning-tree vlan detail	2336
spanning-tree bpdu-guard timeout	2337
spanning-tree extend-system-id	2338
spanning-tree ignore-pvid-inconsistency	2339
spanning-tree link-type	2340
spanning-tree mode	2341
spanning-tree pathcost-type	2343
spanning-tree rpvst-mstp interconnect vlan	2344
spanning-tree tcn-guard	2345
spanning-tree vlan	2345
spanning-tree vlan cost	2347

spanning-tree vlan port-priority	2348
spanning-tree trap	2349
Selftest commands	2351
fastboot	2351
show selftest	2352
sFlow agent commands	2354
clear sflow statistics	2354
sflow	2354
sflow agent-ip	2356
sflow collector	2357
sflow disable	2358
sflow header-size	2358
sflow max-datagram-size	2359
sflow mode	2360
sflow polling	2361
sflow sampling	2362
show sflow	2363
SNMP commands	2366
event-trap-disable	2366
event-trap-enable	2367
lldp trap enable	2367
mac-notify traps	2370
rmon alarm	2372
rmon alarm {enable disable} {index all}	2373
show configuration-changes trap	2374
show mac-notify	2375
show mac-notify port	2376
show rmon alarm	2377
show snmp agent-port	2378
show snmp community	2379
show snmp system	2380
show snmp trap	2381
show snmp views	2382
show snmp vrf	2383
show snmpv3 context	2383
show snmpv3 engine-id	2384
show snmpv3 security-level	2385
show snmpv3 users	2385
snmp-server agent-port	2386
snmp-server community	2387
snmp-server community view	2389
snmp-server historical-counters-monitor	2390
snmp-server response-source	2391
snmp-server snmpv3-only	2393
snmp-server host	2393
snmp-server system-contact	2396
snmp-server system-description	2397
snmp-server system-location	2398
snmp-server trap	2399
snmp-server trap aaa-server-reachability-status	2400
snmp-server trap configuration-changes	2401
snmp-server trap mac-notify	2402
snmp-server trap snmp	2403

snmp-server trap-source interface vrf	2404
snmp-server trap vsx	2405
snmp-server view	2406
snmp-server vrf	2407
snmpv3 context	2408
snmpv3 engine-id	2409
snmpv3 security-level	2410
snmpv3 user	2411
snmpv3 user view	2415
Source-interface selection commands	2417
ip source-interface	2417
ipv6 source-interface <protocol>	2419
ipv6 source-interface dns	2421
show ip source-interface	2422
show ipv6 source-interface	2424
show running-config	2426
SSH client commands	2428
ssh (client login)	2428
SSH client commands	2430
ssh (client login)	2430
SSH server commands	2432
erase ssh sftp-server	2432
show ssh server	2433
show ssh server sessions	2436
show ssh sftp-server usage	2437
ssh ciphers	2438
ssh host-key	2439
ssh host-key-algorithms	2440
ssh key-exchange-algorithms	2441
ssh known-host remove	2443
ssh macs	2444
ssh maximum-auth-attempts	2445
ssh public-key-algorithms	2446
ssh server allow-list	2447
ssh server port	2448
ssh server vrf	2449
ssh sftp-server	2450
show ssh sftp-server file-system	2451
show ssh sftp-server file-system	2452
erase ssh sftp-server	2452
Static routing commands	2454
ip route	2454
ip route bfd	2455
ip route vrf	2457
ipv6 route	2458
show ip rib	2460
show ip rib host-routes	2463
show ipv6 rib	2464
show ipv6 rib host-routes	2466
ipv6 route vrf	2467
show ip route	2469
show ipv6 route	2472

Subinterface commands	2475
encapsulation dot1q	2475
interface	2476
show capacities subinterface	2477
show interface	2478
Supportability copy commands	2480
copy checkpoint	2480
copy command-output	2481
copy core-dump daemon	2482
copy core-dump kernel	2483
copy core-dump kernel <STORAGE-URL>	2484
copy diag-dump feature <FEATURE>	2485
copy diag-dump local-file	2486
copy <IMAGE>	2487
copy running-config	2488
copy show-tech feature	2490
copy show-tech local-file	2491
copy startup-config	2492
copy support-files	2493
copy support-files local-file	2495
copy support-log	2497
Switch system and hardware commands	2499
allow-non-failsafe-updates	2499
bluetooth disable	2500
bluetooth enable	2500
clear events	2501
clear ip errors	2502
console baud-rate	2503
domain-name	2504
hostname	2505
led locator	2506
mtrace	2507
power consumption-average-period	2509
show bluetooth	2509
show boot-history	2511
show capacities	2513
show capacities-status	2514
show console	2515
show core-dump	2516
show deprecated commands	2518
show domain-name	2519
show environment fan	2520
show environment led	2521
show environment power-consumption	2522
show environment power-supply	2525
show environment power-redundancy	2529
show environment temperature	2529
show events	2530
show hostname	2533
show images	2534
show ip errors	2535
show module	2537
show running-config	2539
show running-config current-context	2542

show startup-config	2544
show system	2545
show system resource-utilization	2547
show tech	2551
show usb	2552
show usb file-system	2553
show version	2555
system resource-utilization poll-interval	2556
top cpu	2556
top memory	2557
usb	2558
usb mount unmount	2559
System profile commands	2560
profile	2560
show profiles available	2561
show profile current	2563
Telnet commands	2565
show telnet server	2565
show telnet server sessions	2565
telnet server	2567
Terminal monitor commands	2568
logging console {notify severity filter}	2568
show terminal-monitor	2569
terminal-monitor {notify severity filter}	2570
Traceroute commands	2572
traceroute	2572
traceroute6	2574
Traffic insight commands	2577
monitor type	2577
show capacities traffic-insight	2579
show debug buffer module trafficinsight	2580
show events traffic-insightd	2581
show running-config traffic-insight	2581
show tech traffic-insight	2582
show traffic-insight monitor-type	2583
traffic-insight	2589
TLS commands	2593
cipher-suites 1.2 priority (TLS)	2593
cipher-suites 1.3 priority	2596
key-exchange-algorithms priority	2598
min-version	2601
tls global	2602
show tls	2602
Two-factor authentication commands	2605
aaa authorization radius	2605
https-server authentication certificate	2606
ssh certificate-as-authorized-key	2607
ssh two-factor-authentication	2608

UDLD commands	2610
clear udld statistics	2610
show udld	2610
udld	2612
udld interval	2613
udld mode	2616
udld retries	2617
UFD (Uplink Failure Detection) commands	2619
debug ufd all	2619
delay	2619
links-to-disable	2621
links-to-monitor	2622
ufd enable	2623
ufd session-id	2624
UDP commands	2626
ip forward-protocol udp	2626
ip udp-bcast-forward	2627
show ip forward-protocol udp	2627
User and group commands	2630
password complexity	2630
user	2634
user enable	2637
user disable	2637
user-group	2638
user management-interface	2642
user password	2644
service export-password	2645
show password-complexity	2646
show user-group	2647
show user information	2648
show user-list	2650
show user-list management-interface	2651
VLAN commands	2653
description	2653
vlan name	2653
show capacities-status vlan-count	2654
show capacities svi-count	2655
show capacities vlan-count	2656
show capacities-status vlan-translation	2656
show system internal-vlan-range	2657
show vlan	2658
show vlan port	2659
show vlan summary	2660
show vlan translation	2661
show vlan translation pending	2662
show vlan voice	2663
shutdown	2664
system internal-vlan-range	2665
trunk-dynamic-vlan-include	2666
uufb	2667
vlan	2668

vlan access	2669
vlan protocol	2671
vlan translate	2672
vlan trunk allowed	2674
vlan trunk native	2675
vlan trunk native tag	2676
voice	2677
VRF commands	2679
ip route vrf	2679
ipv6 route gc interval	2680
ipv6 route vrf	2681
show ip route	2682
show ipv6 route	2686
show vrf	2687
vrf	2688
vrf attach	2689
VRRP commands	2691
address	2691
authentication	2692
bfd <IPV4-ADDR>	2694
preempt	2695
preempt delay minimum	2696
priority	2697
router vrrp {enable disable}	2697
no router vrrp	2698
show track	2699
show track brief	2700
show vrrp	2700
shutdown	2708
timers advertise	2709
track (VRRP group)	2710
track (VRRP virtual router)	2711
track by	2712
version	2713
vrrp	2713
vrrp dual-active-forwarding	2714
VSX commands	2716
active-gateway	2716
config-sync disable	2721
inter-switch-link {<PORT-NUM> lag <LAG-ID>}	2721
inter-switch-link dead-interval	2722
inter-switch-link hello-interval	2723
inter-switch-link hold-time	2724
inter-switch-link peer-detect-interval	2725
interface lag multi-chassis	2726
ip icmp redirect	2727
keepalive dead-interval	2728
keepalive hello-interval	2729
keepalive peer	2730
keepalive udp-port	2731
lacp fallback	2732
linkup-delay-timer	2733
linkup-delay-timer exclude lag-list	2734

neighbor <IP-ADDRESS> vsx-sync-exclude	2735
role {primary secondary}	2736
show active-gateway	2737
show active-gateway <IFNAME>	2739
show interface <VLAN-NAME>	2740
show lacp aggregates	2741
show lacp interfaces	2742
show lacp interfaces multi-chassis	2745
show running-config interface	2746
show running-config vsx	2747
show running-config vsx-sync	2748
show running-config vsx-sync peer-diff	2749
show vsx active-forwarding	2750
show vsx brief	2751
show vsx config-consistency	2753
show vsx config-consistency lacp	2754
show vsx configuration	2756
show vsx configuration split-recovery	2757
show vsx ip data-path	2758
show vsx ip route	2760
show vsx ipv6 data-path	2762
show vsx ipv6 route	2763
show vsx status	2765
show vsx status config-sync	2769
show vsx status peering	2769
show vsx status shutdown-on-split	2770
split recovery	2771
system-mac	2772
vsx	2773
vsx active-forwarding	2774
vsx shutdown-on-split	2775
vsx-sync	2776
vsx-sync (config-if, config-lag-if contexts)	2780
vsx-sync (config-vlan-if context)	2784
vsx-sync aaa	2785
vsx-sync acl-log-timer	2786
vsx-sync acl-secure-update	2787
vsx-sync bfd-global	2788
vsx-sync bgp	2789
vsx-sync copp-policy	2790
vsx-sync dcb-global	2791
vsx-sync dhcp-relay	2792
vsx-sync dhcp-server	2793
vsx-sync dhcpv6-server	2794
vsx-sync dns	2795
vsx-sync evpn	2796
vsx-sync icmp-tcp	2797
vsx-sync keychain	2798
vsx-sync lldp	2799
vsx-sync loop-protect-global	2800
vsx-sync mclag-interfaces	2800
vsx-sync nd-snooping	2802
vsx-sync neighbor	2803
vsx-sync ospf	2804
vsx-sync policy-global	2805
vsx-sync qos-global	2806

vsx-sync route-map	2807
vsx-sync sflow	2808
vsx-sync sflow-global	2809
vsx-sync snmp	2810
vsx-sync ssh	2810
vsx-sync static-routes	2811
vsx-sync stp-global	2812
vsx-sync telnet	2814
vsx-sync time	2814
vsx-sync udp-forwarder	2815
vsx-sync vrrp	2816
vsx-sync vsx-global	2817
vsx update-software	2818
vsx update-software boot-bank	2820
VXLAN commands	2822
interface vxlan	2822
routing	2823
show interface vxlan	2824
show interface vxlan multipoint-tunnel	2825
show interface vxlan vni	2828
show interface vxlan vteps	2829
shutdown	2834
source ip	2835
vlan	2836
vni	2837
vrf	2838
vtep-peer	2839
vxlan-counters aggregate	2840
Zeroization commands	2842
erase all zeroize	2842
ZTP commands	2845
show ztp information	2845
ztp force provision	2848
Support and Other Resources	2851
Accessing HPE Aruba Networking Support	2851
Accessing Updates	2852
Warranty Information	2852
Regulatory Information	2852
Documentation Feedback	2852

Chapter 1

About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing HPE Aruba Networking switches on a network.

Applicable products

This document applies to the following products:

- HPE Aruba Networking 9300 Switch Series (R9A29A, R9A30A, R8Z96A, S0F81A, S0F82A, S0F83A)
- HPE Aruba Networking 9300S Switch Series (S0F81A, S0F82A, S0F83A, S0F84A, S0F85A, S0F86A, S0F88A, S0F95A, S0F96A)

What's new in this release

The following commands were added or modified in AOS-CX 10.17.



For more information on new features introduced in this release, visit the [HPE Aruba Networking AOS-CX Software Release Technical Update](#) channel on YouTube.

Commands introduced or modified in 10.17

Command	Description
arp-suppression {enable disable}	Enables ARP suppression for EVPN-VxLAN on specific VLAN.
arp-suppression exclude	This command exempts certain IP addresses from ARP suppression and allows ARP requests for those IP addresses to be flooded across the VxLAN fabric.
crypto pki application gnmi certificate	Configures a certificate for the gNMI server.
dhcp-relay option 82	The circuit-id port-id parameter was introduced. This parameter configures the circuit ID and remote ID options.
dhcp-relay vsx active-active	Enables DHCP relay active-active mode in VSX.
dhcpv6-relay vsx active-active	Enables DHCPv6 relay active-active mode in VSX.
dhcpv4 relay	The following command outputs were updated to introduce circuit ID and remote ID information. ▪ show dhcp-relay

Command	Description
	▪ diag-dump dhcp-relay basic
dhcpv6 relay	The following command outputs were updated to introduce circuit ID and remote ID information. ▪ show dhcpv6-relay ▪ diag-dump dhcpv6-relay basic
gnmi vrf	Enables the gNMI server on a given VRF.
gateway-bd (IPv4)	Enables multicast interconnectivity between EVPN PE routers and PIM routers in EVPN VXLAN networks by using a Gateway Bridge Domain (Gateway BD).
gateway-bd (IPv6)	Enables multicast interconnectivity between EVPN PE routers and PIM routers in EVPN VXLAN networks by using a Gateway Bridge Domain (Gateway BD).
ip dns fqdn-resolver force-refresh	This command initiates a force refresh for FQDN resolver entry/entries.
ip dns fqdn-resolver refresh-interval	Sets the refresh interval for FQDN resolvers. The interval specifies the time in seconds after which the FQDN resolver entries are refreshed.
ip pim-sparse accept-remote-source (IPv4)	Enables the router to accept multicast traffic from remote sources.
ipv6 pim6-sparse accept-remote-source (IPv6)	Enables the router to accept multicast traffic from remote sources.
ip route bfd	The name parameter was added. This parameter allows you to assign a name to the destination route.
ip ipv6 vrf	The name parameter was added. This parameter allows you to assign a name to the destination route.
monitor type	The dropped-flows flow monitor type is available on 5420, 6200, 8100, 8360 and 9300 Switch series.
multicast-replication-mode oism	Allows inter-subnet IP multicast traffic to be routed among L2 VNIs. EVPN Optimized Inter-Subnet Multicast (OISM) is a standard defined in RFC9625. In deployments using PIM over VXLAN, multicast routing is achieved by exchanging PIM control packets over VXLAN tunnels.
nd-suppression (enable disable)	This command enables ND suppression for EVPN-VxLAN on specific VLAN.
nd-suppression exclude (per VLAN)	This command exempts certain IPv6 addresses from ND suppression and allows neighbor solicitation (NS) for those IPv6 addresses to be flooded across the VXLAN fabric even though the target addresses are present in the NDMD cache.
packet-capture commands	The following Packet Capture commands were introduced in AOS-CX 10.17: ▪ packet-capture ▪ packet-capture enable ▪ show packet-capture session

Command	Description
	▪ show packet-capture pcaps ▪ packet-capture delete-pcap ▪ copy packet-capture
persona custom	Assigns a persona LAG to a LAG interface. The persona LAG is used to apply a common configuration to multiple LAGs. There are two modes for applying a persona LAG: copy and attach .
show interface persona	Shows all interface personas and their attached interfaces.
interface persona lag	Creates a persona LAG, a template for LAG interfaces. A persona LAG defines configuration options that can be applied to multiple LAGs for consistency and simplified management. Only LAG interfaces can reference persona LAG templates. The persona LAG name cannot use reserved interface names or formats, such as vlan, lag, or loopback. Configurations defined in a persona LAG are valid only for LAG interfaces.
queue-monitor polling-interval seconds	Configures the polling interval used to sample interface queue data. The specified interval is applied to all interfaces where queue monitoring is enabled. Changing the polling interval clears all previously collected queue statistics and restarts data collection from the time the new interval is applied.
remote AAA	The key length for the plaintext value in the key parameter was increased from 32 to 128 characters in the following commands: ▪ radius-server host ▪ radius-server host secure ipsec ▪ tacacs-server host ▪ tacacs-server key
show evpn oism	Displays the status and configuration details of OISM in the EVPN network.
show ip dns fqdn-resolver	This command displays a summary table of all FQDN resolver entries, including the total count of FQDN entries, refresh time, source information, and a tabular display of all entries.
show gnmi	Displays the current gNMI configuration.
show interface queue-monitor status	Displays the queue monitoring status for a specific interface or range of interfaces. If no interface is specified, the command will display the queue monitoring status for all interfaces configured.
show ip dns fqdn-resolver detail	Displays detailed hierarchical information for FQDN resolver entries, including the FQDN, VRF, requested address family, resolved IPv4 and IPv6 addresses, resolution status, and remaining refresh timer.
show ip dns fqdn-resolver refresh-interval	Displays the current refresh interval for FQDN resolvers.
show system resource-utilization	Memory usage was added to the outputs of the standby and member parameters.
show traffic-insight monitor-type	Introduces congested-flows monitor type.

Command	Description
static route	The name parameter was added to the following commands. This parameter allows you to assign a name to the destination route: ▪ ip route ▪ ipv6 route
supplementary-broadcast-domain	Configures a given VLAN as a Supplementary Broadcast Domain (SBD). In a VXLAN-EVPN network, only one VLAN per VRF can be configured as an SBD. EVPN Route Type-6 joins on the client VLAN are translated to the SBD VLAN, and the remote VTEP learns the join on the SBD VLAN.
vrf	The name parameter was added to the following commands. This parameter allows you to assign a name to the destination route: ▪ ip route vrf ▪ ipv6 route vrf
show ip dhcp preferred-vlan	Displays the preferred DHCP client VLANs configured on the system.
ip dhcp preferred-vlan	Specifies the preferred VLAN for DHCP client options, including DNS, NTP, and Default Gateway.
ip dhcp	Support has been enabled on one or more user VLANs.
ipv6 dhcp	Support has been added for DHCPv6 on multiple VLANs.
bgp bestpath bgp-std-selection	Configures the standard Border Gateway Protocol (BGP) best-path selection process used by major vendors.
diag persistent-storage	Enables or disables storage of logs in storage.
logging persistent-storage	Enables or disables storage of logs in storage.
apply access-list (to subinterface)	Command introduced on the 9300 and 9300S Switch Series.
show access-list hitcounts	Added support for L3 VNI ACLs on the 9300 and 9300S Switch Series.

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in [Support and Other Resources](#).

Command syntax notation conventions

Convention	Usage
<code>example-text</code>	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets ([]).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ▪ <code><example-text></code> ▪ <code><example-text></code> ▪ <code>example-text</code> ▪ <code>example-text</code>	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ▪ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value. ▪ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[]	Brackets. Indicates that the enclosed item or items are optional.
... or ...	Ellipsis: ▪ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ▪ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term **switch**, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

```
switch (CONTEXT-NAME) #
```


Indicates the configuration context for a feature. For example:

```
switch(config-if) #
```

Identifies the **interface** context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100) #
```

When referring to this context, this document uses the syntax:

```
switch(config-vlan-<VLAN-ID>) #
```

Where *<VLAN-ID>* is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format: ***member/slot/port***.

On the HPE Aruba Networking 8xxx, 93xx, and 10xxx Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface **1/1/4** in software is associated with physical port 4 on the switch.



If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

CLI access

Access the CLI through the following interfaces:

Console port

Connect the management port on the switch to your computer using a serial cable and then use terminal emulation software to reach the switch from the computer. Typically, the console port is used when first installing the switch and performing initial configuration tasks.

Management port (out-of-band connection)

Connect the management port on the switch to your network, and then use SSH client software to reach the switch from a computer connected to the same network. This requires that a DHCP server is installed on the network.

In the switch factory default state, the management port and SSH on the management VRF (**mgmt**) are enabled.

Data port (in-band connection)

Connect a data port on the switch to your network, and then use SSH client software to reach the switch from a computer connected to the same network. Management traffic ingresses and egresses switch data ports with rest of the traffic on the network, therefore it can be affected by traffic congestion and other issues impacting the network.

Getting CLI help

To show the available commands that you can execute in the current command context, enter the **?** symbol.

For example:

```
switch# ?
  boot           Reboot all or part of the system
  checkpoint      Checkpoint information
switch#
```

The **?** symbol does not display on the screen when you enter it.

The commands that are available to you depend on your authority and the command context. In a given command context, you can only list and execute the commands available in that context.

To show the available parameters for a command, enter the command followed by a space and then enter the **?** symbol.

For example:

```
switch(config)# access-list ?
  all          All access-lists
  ip           Internet Protocol v4 (IPv4)
  ipv6         Internet Protocol v6 (IPv6)
  log-timer    Set ACL log timer length (frequency)
  mac          Ethernet MAC Protocol
switch(config)# access-list
```

After the CLI displays the information, it automatically displays the text you entered before you entered the **?** symbol.

If there is no **<cr>** symbol at the end of the command help output, the command is not complete as displayed. You must specify one of the listed parameters.

The **<cr>** symbol alone in the command help output indicates that there are no additional parameters and that you must press the enter key to complete the command. For example:

```
switch# list ?
  <cr>
switch# list
```

The **<cr>** symbol at the end of the command help output indicates that the parameters preceding the **<cr>** are optional and you can enter the command as is displayed. For example:

```
switch# configure ?
  terminal     Configuration terminal (default)
  <cr>
switch# configure
```

To show information about a parameter for a command, enter the command and parameter followed by a space, then enter the **?** symbol.

For example:

```
switch(config)# access-list log-timer ?
  <30-300>     Specify value (in seconds)
  default      Default value (300 seconds)
switch(config)# access-list log-timer
```

Authority levels

In command descriptions, the authority level indicates the user role that is required to execute a command:

Administrators

Users with the role: **administrators**

Users with administrator rights can execute any command.

Operators

Users with the role: **operators**.

Users with operator rights can execute commands in the operator context (**>**) only.

Auditors

Users with the role: **auditors**.

Users with auditor rights can execute commands in the auditor context (**auditor>**) only.

Local user group members with execution rights for a command

You can create up to 29 user-defined local user groups on the switch. Each group can be defined to allow execution of up to 1024 specific CLI commands.

Command contexts

The command context determines the following:

- Which parts of the switch can be managed
- Which commands are available to users with the appropriate authority

Command contexts have a parent-child tree structure in which contexts might themselves contain nested contexts.

Operator context (>)

The operator context enables you to execute commands to view—but not change—the configuration.

The operator context requires the least user privilege to execute commands.

In command descriptions, this context is listed as: Operator (>)

Switch prompt example

```
switch>
```

Authority

Operators or Administrators

Showing the available commands in this context

At the command prompt, enter the ? symbol.

Navigating to the operator context (>)

To navigate to the operator command context (>), do one of the following:

- Log in to the switch CLI with a user ID that has the **operator-group** role.
- From the manager context (#), enter the **disable** command.

Auditor context

When you log in to the switch as user with auditor rights, you have access to the auditor command context only.

Users with auditor rights have access to a limited set of commands. for more information about auditors, see the *Security Guide* for your switch and software version.

Switch prompt example

```
auditor>
```

Showing the available commands in this context

At the command prompt, enter the ? symbol.

Manager context (#)

From the manager context (#), you can execute commands that do not require saving changes to the configuration.

In command descriptions, this context is listed as: Manager (#)

Switch prompt example

switch#

Authority

Administrators or local user group members with execution rights for this command.

Showing the available commands in this context

At the command prompt, enter the **?** symbol.

Access to manager context commands from descendant contexts

The **do** command enables you to access commands from the manager context while you are in a child or descendent context, such as **config** or **config-if**.

For example, to execute the **clear** command from the **config** context, enter the following: **do clear**.

The **show** command can be executed from configuration contexts as well as the manager context, so using the **do** command with the **show** command is deprecated. Support for **do show** might be discontinued in a future software release.

Navigating to the manager context (#)

To navigate to the manager command context (#), do one of the following:

- Log in to the switch CLI with a user ID that has the **administrators** role.
- From the operator context (>), enter the **enable** command.

You must have administrator authority to enter the **enable** command.

```
switch> enable
switch#
```

- From the configuration context (**config**), enter either the **exit** or the **end** command.

For example:

```
switch(config)# exit
switch#
```

- From any child or descendent context, enter the **end** command.

For example:

```
switch(config-vlan-100)# end
switch#
```

Global configuration context (config)

From the global configuration context (**config**), you can execute commands that change the configuration of the switch.

In command descriptions, this context is listed as: **config**

Switch prompt example

switch(config)#

Authority

Administrators or local user group members with execution rights for this command.

Showing the available commands in this context

At the command prompt, enter the **?** symbol.



You can use the **do** command to execute some manager context commands—such as the **clear** command—from the global configuration context.

Navigating to the config context

To navigate to the **config** command context, do one of the following:

- From the manager context (**#**), enter the **configure terminal** command:

```
switch# configure terminal
switch(config)#
```

- From a child configuration context, enter the **exit** command.

For example:

```
switch(config-vlan-100)# exit
switch(config)#
```

Other configuration command contexts

All other configuration command contexts are descendants of the global configuration command context (**config**).

From these command contexts, you can execute commands that apply to that specific context, such as an interface or a VLAN.

Switch prompt examples

- **switch(config-if)#**
- **switch(config-router)#**
- **switch(config-vlan-100)#**

Authority

Administrators or local user group members with execution rights for this command.

Showing the available commands in this context

At the command prompt, enter the **?** symbol.

Support for range contexts

Some switch features enable you to use a single command to apply configuration settings to multiple items. You specify the multiple items by creating a type of command context called a **range context**. Then you can execute commands that are applied to every item in the range. For example:

```
switch(config)# interface 1/1/1-1/1/5  
switch(config-if-<1/1/1-1/1/5>)# no shutdown
```

You can use a range context to specify multiple items for the following:

Physical interfaces

- Command example: **interface 1/1/1-1/1/8,1/1/10,1/1/12**
- Switch prompt example: **switch(config-if-<1/1/1-1/1/8,1/1/10,1/1/12>)#**

LAG interfaces

- Command example: **interface lag 1-10**
- Switch prompt example: **switch(config-if-lag-<1-10>)#**

Loopback interfaces

- Command example: **interface loopback 1-10**
- Switch prompt example: **switch(config-if-loopback-<1-10>)#**

VLAN interfaces

- Command example: **interface vlan 1,2,3-6**
- Switch prompt example: **switch(config-vlan-if-<1,2,3-6>)#**

VLANs

- Command example: **vlan 1-10,15,20-25**
- Switch prompt example: **switch(config-vlan-<1-10,15,20-25>)#**

Commands entered in a range context are applied to each item in the range individually:

- Each item in the range has its own entry in the output of **show running-config** commands. For example, you can configure a range of interfaces as follows:

```
switch(config)# interface 1/1/1-1/1/5  
switch(config-if-<1/1/1-1/1/5>)# no shutdown
```

In the output for the show running-config command, the interfaces are displayed individually:

```
switch(config-if-<1/1/1-1/1/5>)# show running-config  
Current configuration:  
...  
interface 1/1/1  
    no shutdown  
interface 1/1/2
```

```

        no shutdown
interface 1/1/3
        no shutdown
interface 1/1/4
        no shutdown
interface 1/1/5
        no shutdown
...
switch(config-if-<1/1/1-1/1/5>)#

```

- If you specify a range context for interfaces, you cannot execute commands that create a context within the range context. For example, you cannot execute the **vrrp** command from an interface range context, even though you can execute the command from the **config-if** context for a single interface.
- If error is encountered during the execution of a command for an item in the range, the error message returned includes a prefix that identifies the item to which the error applies. However command execution does not stop until the command is attempted on all the items in the range. For example, attempting to set an IP address in a range context of loopback interfaces results in the IP address being applied to the first loopback interface in the range, but results in errors for the subsequent interfaces:

```

switch(config)# interface loopback 1-4
switch(config-loopback-if-<1-4>)# ip address 10.1.11.11/24
[loopback2] Overlapping networks observed for "10.1.11.11/24". Please configure
non overlapping networks.
[loopback3] Overlapping networks observed for "10.1.11.11/24". Please configure
non overlapping networks.
[loopback4] Overlapping networks observed for "10.1.11.11/24". Please configure
non overlapping networks.

switch(config-loopback-if-<1-4>)# show running-config | begin 4 "loopback 1"
interface loopback 1
    ip address 10.1.11.11/24
interface loopback 2
interface loopback 3
interface loopback 4

```

- The range context is created only if every item in the range is successfully created or already exists in configuration. If an error occurs during the creation of an item in a range, the items that are created successfully are added to the configuration, but the range context is not created. The switch prompt. For example, in the following sequence:
 1. VLANs 1 through 100 are created successfully, so the switch prompt reflects the range of VLANs: **switch(config-vlan-<1-100>)#**
 2. The command **interface vlan 95-105** fails for VLANs 101 through 105, so the range context is not created and the switch prompt remains in the global configuration context: **switch (config)#**
 3. The configuration includes all the VLANs and VLAN interfaces that are created successfully.

```

switch(config)# vlan 1-100
switch(config-vlan-<1-100>)# exit

```



```

switch(config)# interface vlan 95-105
VLAN 101 should be created before creating interface VLAN101.
VLAN 102 should be created before creating interface VLAN102.
VLAN 103 should be created before creating interface VLAN103.
VLAN 104 should be created before creating interface VLAN104.
VLAN 105 should be created before creating interface VLAN105.
switch(config)# show running-config
Current configuration:
...
vlan 1-100
interface vlan95
interface vlan96
interface vlan97
interface vlan98
interface vlan99
interface vlan100
...
switch(config)#

```

- If the **no** form of the command can be used to remove an item from the configuration, you can use a range context with the **no** form of the command to remove multiple items from the configuration. For example, you can remove VLANs 95 through 100 from the configuration by entering: **no vlan 95-100**

Rules for range contexts

For interfaces that use the **member/slot/port** notation, items in the range must be specified in ascending order. The switch prompt is truncated to 50 characters.

Contiguous items in the range are represented by the smallest and largest values separated by a hyphen. For example:

Command: **interface 1/1/1-1/1/8**

Switch prompt: **switch(config-if-<1/1/1-1/1/8>)#**

Command: **vlan 1-10**

Switch prompt: **switch(config-vlan-<1-10>)#**

Noncontiguous items in the range must be separated by commas. For example:

Command: **interface 1/1/1-1/1/8,1/1/10,1/1/12**

Switch prompt: **switch(config-if-<1/1/1-1/1/8,1/1/10,1/1/12>)#**

Command: **vlan 1-10,15,20-25**

Switch prompt: **switch(config-vlan-<1-10,15,20-25>)#**

Command history

You can use the **up arrow** key or **Ctrl+P** to display the previous command in the session history, if any.

You can use the **down arrow** key or **Ctrl+N** to display the next command in the session history, if any.

You can use the **show history** command to show a numbered list of the commands executed during this session. You use the command numbers to specify commands to repeat using the **repeat** command. The **show history** and **repeat** commands are not saved in the history buffer.

The commands saved in the history command buffer are in the same format in which you entered the commands. If you enter an incomplete command, the command saved in the history command buffer is also an incomplete one.

If you execute the same command repeatedly, the switch saves only the earliest record. However, if you execute the same command in different formats, the switch saves them as different commands.

For example, if you execute the **show startup-config** command repeatedly, the system saves only one command in the history command buffer. If you execute the command in the format of **show start** and **show startup** respectively, the system saves them as two commands.

Command completion

The CLI supports both command abbreviation and command completion:

- If you enter enough letters to match a valid command, the CLI accepts the command.
For example, you can enter **con** instead of **configure** to navigate from the manager context to the global configuration context.

```
switch# con
switch(config)#
```

- If you enter part of a command word and then press the **Tab** key, one of the following occurs:
 - If you have entered enough letters to match a valid command, the CLI displays the remainder of the word.
 - If you have not entered enough letters to match a valid command, the CLI does not complete the command.

If you press the **Tab** key a second time, the CLI displays commands that match the letters you entered.

For example:

```
switch(config)# cl
class clear clock
switch(config)# cl
```

- If you press the **Tab** key twice after a completed word, the CLI displays the command options.
For example, if you enter the word **clock** followed by a space and then press the **Tab** key twice, the CLI displays the commands available in that command context that start with that word, and then displays the prompt—including the characters you entered—enabling you to complete the command without retyping.

```
switch(config)# clock
date      datetime      time    timezone
switch(config)# clock
```

Pipe (|) support in show commands

The pipe (|) command is a CLI session command that filters the output of show **show** commands according to the criteria specified by the parameter **include**, **exclude**, **count**, **begin**, or **redirect**.

- The pipe (|) command is supported for use with the **show** command only.
- You can use multiple pipe commands with a single show command.
For example: **show running-config | include "vlan" | exclude "vlan2" | count**
- You can use the pipe command with the **page** command.
- Command completion by pressing the **Tab** key is not supported for pipe commands.

Command syntax notation conventions

Convention	Usage
<code>example-text</code>	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets ([]).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ▪ <code><example-text></code> ▪ <code><example-text></code> ▪ <i>example-text</i> ▪ <i>example-text</i>	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ▪ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value. ▪ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[]	Brackets. Indicates that the enclosed item or items are optional.
... or ...	Ellipsis: ▪ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ▪ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

boot

boot

Description

Presents you with the boot menu prompt. You can then specify which boot profile: primary, secondary, or Service OS console.

Example

Presenting the boot menu prompt:



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

cat

cat <FILENAME/DIRECTORY-NAME>

Description

Prints the contents of a file to the console. The Service OS does not allow command output redirection, so this command is only useful for reading short text files.

Parameter	Description
<FILENAME/DIRECTORY-NAME>	Shows the contents of the specified file or directory.

Example

Showing the contents of /nos/hosts:

```
SVOS> cat /nos/hosts
127.0.0.1      localhost.localdomain      localhost

SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

cd path

cd path

Description

Changes the current working directory.

Example

Changing the current working directory:

```
cd /
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

config-clear

config-clear

Description

Configures the switch to set all configuration settings to factory default when the switch is restarted. The next time the switch starts, the current **startup-config** is renamed to **startup-config-fixme**, and a new **startup-config** is created with factory default settings.



Using this command is not the same as performing zeroization, which securely erases the entire primary storage and other devices, and not just the configuration.

Example

Configuring the system to clear the switch configuration:

```
SVOS> config-clear

The switch configuration will be cleared.

Continue (y/n)? y
The system has been configured to clear the startup-config on the next
boot. Please execute the 'boot' command to complete this action.
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

cp

cp [options] <SOURCE-FILENAME/SOURCE-DIRECTORY> <DESTINATION-FILENAME/DESTINATION-DIRECTORY>

Description

Copies files or directories.

Parameter	Description
[options]	Selects the options for the command.
-d, -P	Specifies the preservation of symlinks (default if -R).
-a	Same as -dpR .
R, -r	Specifies recursiveness, all files, and subdirectories are copied.
-L	Specifies the following of all symlinks.
-H	Specifies the following of symlinks on command line.
-p	Specifies the preservation of file attributes if possible.
-f	Specifies the overwriting of a file or directory.
-i	Specifies the prompting before an overwrite.
-l, -s	Specifies the creation of (sym) links.
<SOURCE-FILENAME/SOURCE-DIRECTORY>	Specifies the name of the source file or directory.
<DESTINATION-FILENAME/DESTINATION-DIRECTORY>	Specifies the name of the destination file or directory.

Example

Copying /home/customers directory to the /home/clients directory:

```
SVOS> cp /home/customers /home/clients
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (SVOS>)	Administrators or local user group members with execution rights for this command.

du

du [options] <FILENAME/DIRECTORY-NAME>...

Description

Shows estimated disk space used for each file or directory or both.

Parameter	Description
[options]	Selects the options for the command.
-a	Show file sizes.
-L	Shows all symlinks.
-H	Shows symlinks on a command line.
-d, N	Shows limited output to directories (and files with -a) of depth less than N .
-c	Shows the total disk space usage of all files or directories or both.
-l	Shows the count sizes if hard linked.
-s	Shows only a total for each argument.
-x	Does not show directories on different file systems.
-h	Show sizes in human readable format (1K, 243M, and 2G).
-m	Show sizes in megabytes.
-k	Show sizes in kilobytes (default).
<FILENAME/DIRECTORY-NAME>	Specifies the file or directory or both for displaying a size estimate.

Example

Estimating disk space for the /nos directory:

```
SVOS> du -ah /nos
196.4M /nos/primary.swi
196.4M /nos
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

erase zeroize

erase zeroize

Description

Securely erases any user data contained on the SSD or other storage devices on the management module.



Back up all data before running this command or all user/config data will be lost.

Usage

Use this command to securely erase all customer data and restore the software environment to factory default. When you issue this command:

- Software images are copied to RAM to be restored on completion.
- All bits undergo a 0>1>0 transition to completely zeroize data. This data is not recoverable.
- This feature can be used to remove all configuration settings or system alterations for debugging or troubleshooting.
- The zeroization process takes approximately two minutes.



All logs and data are lost in the zeroization process. Best practices is to collect all applicable data before performing zeroization.

Example

Erasing user data:

```
SVOS> SVOS> erase --help
Usage: erase zeroize

Securely erases storage devices on the management module.
SVOS>
...

...

SVOS> erase zeroize
#####WARNING#####
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
```

```

switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
#####WARNING#####

Continue (y/n)? y
reboot: Restarting system

##### Preparing for zeroization #####

##### Storage zeroization #####
##### WARNING: DO NOT POWER OFF UNTIL #####
##### ZEROIZATION IS COMPLETE #####
##### This should take several minutes #####
##### to one hour to complete #####

##### Restoring files #####

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

exit

exit

Description

Logs the user out from the svos> prompt.

Example

Logging the user out from the svos> prompt:

```

SVOS> exit

(C) Copyright 2025 Hewlett Packard Enterprise Development LP

RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software

```

Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

To reboot without logging in, enter 'reboot' as the login user name.

ServiceOS login:



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

format

format

Description

Configures the primary storage device with the correct partition and file system formatting. This command removes all pre-existing data on the primary storage device.

Example

Configuring the primary storage device with the correct partition and file system formatting:

```
SVOS> format
#####WARNING#####
The following action will cause all data on
the primary storage device to be lost. After
formatting has completed, a reboot will be
initiated to complete storage initialization.
#####WARNING#####

Continue? (y/n): y

Working...This may take a few minutes...
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

identify

identify

Description

Prints the version of the SVOS and of the UEFI BIOS.

Example

Output from a 9300 switch:

```
SVOS> identify
mc svos_primary      : CL.01.01.0004
mc svos_secondary    : CL.01.01.0004
mc uefi               : CL-01-0010
mc uefi_capsule       : CL-01-0010
Support Info         : SE:0
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

ip

ip {show | dhcp | disable | addr <ADDR-NETMASK-GATEWAY>}

Description

Shows or configures the port with a static IP address (IPv4 only) or enables the DHCP client on the port. An address is set only if a DHCP server is available to provide one.

Parameter	Description
{show dhcp disable addr <ADDR-NETMASK-GATEWAY>}	Selects the options for the OOBM port.
show	Shows the OOBM port.
dhcp	Configures the port with a DHCP address.
disable	Disables the OOBM port.
addr <ADDR-NETMASK-GATEWAY>	Configures the port with a static IP address (IPv4 only). Specify address, netmask, and gateway as A.B.C.D.

Example

Configuring the port with a DHCP IP address:

```
SVOS> ip dhcp
SVOS> ip show
Interface   : Link Up
IP Address  : 10.0.26.17
Subnet Mask: 255.255.252.0
Gateway     : 10.0.24.1

SVOS> ip disable
SVOS> ip show
Interface   : Disabled
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

ls

ls [<OPTIONS>] [<FILE-NME>]

Description

This command lists directory contents.

Parameter	Description
<OPTIONS>	Specifies options for the command.
-l	Shows one-column output.
-a	Shows entries which start with a period (.).
-A	Shows output similar to -a , but excludes a period (.) and a double period (..).
-C	Shows output list by columns.
-x	Shows output list by lines.
-d	Shows listing of directory entries instead of contents
-L	Follows symlinks.
-H	Follows symlinks on the command line.
-R	Recurse.
-p	Appends a slash (/) to directory entries.
-F	Appends an indicator to entries. An indicator can be as an asterisk (*) or slash (/) or equal sign (=) or at sign (@) or pipe ().
-l	Shows the output in a long listing format.
-i	Shows the list inode numbers.
-n	Shows a list of numeric UIDs and GIDs instead of names.
-s	Shows a list of allocated blocks.
-e	Shows in one column a list with the full date and time.
-h	Shows list sizes in human readable format (1K, 243M, 2G) with a one-column output.
-r	Shows in one column a sort in reverse order.
-S	Shows in one column a sort by size.
-X	Shows in the output sort by extension.
-v	Shows in one column a sort by version.
-c	With -l , it shows a sort in one column by ctime .
-t	With -l , it shows a sort by mtime .
-u	With -l , sort by atime .

Parameter	Description
-c	With -l, it shows a sort in one column by ctime
-w <N>	Assumes that the terminal has the number of columns wide as specified by <N>.
--color[={always never auto}]	Controls color in the output.
<FILE-NAME>	Specifies the name of the file to list.

Example

Listing directory contents:

```
SVOS> ls -la /nos
drwxr-xr-x   3 0      0      4096 Nov 21 03:19 .
drwxr-xr-x  11 0      0      220 Nov 21 03:21 ..
drwx-----   2 0      0     16384 Nov 21 03:20 lost+found
-rwxr-xr-x   1 0      0    205957424 Nov 21 03:19 primary.swi
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

md5sum

md5sum [-c | -s | -w] [<FILE-NAME>]

Description

This command computes and checks the MD5 message digest.

Parameter	Description
[-c -s -w]	Selects the options for the command.
-c	Specifies to check the sums against the list in files.

Parameter	Description
-s	Specifies not output anything, status code shows success.
-w	Specifies to warn about improperly formatted checksum lines.
<FILE-NAME>	Specifies the file name to run the checksum against.

Example

Computing and checking the MD5 message digest for /nos/primary.swi:

```
SVOS> md5sum /nos/primary.swi
93ffc89e7ec357854704d8e450c4b7ab /nos/primary.swi
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

mkdir

mkdir [-m | -p] [<DIRECTORY-NAME>]

Description

This command makes directories.

Parameter	Description
[-m -p]	Specifies the options for the command.
-m	Specifies the mode.
-p	Specifies to make parent directories as needed with no errors for pre-existing directories.
<DIRECTORY-NAME>	Specifies the directory to create.

Example

Making the dir directory:

```
SVOS> mkdir dir
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

mount

mount <DEVICE>

Description

This command mounts the SSD partitions to the following locations: **/coredump**, **/logs**, **/nos**, **/selftest**, and mounts the USB device to **/mnt/usb**.

Users can mount USB flash drives formatted as either FAT16 or FAT32 with a single partition.

Parameter	Description
<DEVICE>	Specifies the device to be mounted. Supported device options include <code>all</code> and <code>usb</code> .

Examples

Mounting all of the SSD partitions:

```
SVOS> mount all
SVOS> mount usb
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

mv

`mv [-f | -i | -n] <TARGET-DIRECTORY>`

Description

This command moves (renames) files.

Parameter	Description
-f	Specifies not to prompt before overwriting.
-i	Specifies to prompt before overwriting.
-n	Specifies to not overwrite an existing file.

Example

Moving the file named myfile:

```
svos> mv myfile
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

password (svos)

password

Description

Sets the admin user account password for both Service OS and AOS-CX once the user boots into AOS-CX and saves the configuration. This will overwrite the previous password if one exists. User input is masked with asterisks.

This command is not available if enhanced secure mode is set.

Example

Setting the admin account password:

```
SVOS> password
Enter password:*****
Confirm password:*****
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

ping

ping <HOST-IP-ADDRESS>

Description

Pings network hosts for debug purposes.

Parameter	Description
<HOST-IP-ADDRESS>	Specifies the host IP address.

Example

Pinging a network host:

```
SVOS> ping 10.0.8.10
PING 10.0.8.10 (10.0.8.10): 56 data bytes
64 bytes from 10.0.8.10: seq=0 ttl=63 time=3.496 ms
64 bytes from 10.0.8.10: seq=1 ttl=63 time=0.367 ms
64 bytes from 10.0.8.10: seq=2 ttl=63 time=0.380 ms
64 bytes from 10.0.8.10: seq=3 ttl=63 time=0.282 ms
64 bytes from 10.0.8.10: seq=4 ttl=63 time=0.669 ms
^C
--- 10.0.8.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.282/1.038/3.496 ms
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

pwd

pwd

Description

Displays the current working directory.

Example

Displaying the current working directory:

```
SVOS> pwd
/home
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

reboot

reboot

Description

Reboots the Management Module.

Example

Rebooting the management module:

```
SVOS> reboot
reboot: Restarting system
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

rm

rm [-f | -i | -R | -r] <FILE-NAME>

Description

Removes files or directories.

Parameter	Description
<code>[-f -i -R -r]</code>	Selects the options for removing files or directories.
<code>-f</code>	Never prompt before removing files or directories.
<code>-i</code>	Always prompt before removing files or directories.
<code>-R -r</code>	Recursive.

Example

Removing the file named **foo**:

```
SVOS> rm foo
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

rmdir

```
rmdir [-p] <DIRECTORY-NAME>
```

Description

Removes empty directories.

Parameter	Description
<code>-p</code>	Specifies to remove parent directories.

Example

Removing the empty **foo** directory:

```
SVOS> rmdir foo
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

secure-mode

`secure-mode <enhanced | standard | status>`

Description

Sets the secure mode to enhanced or standard secure mode. Also can display the current secure mode. A zeroization is required before switching between enhanced and standard secure modes.

The command also displays a message notifying the user that they are already in the targeted secure mode.

Example

Setting the secure mode to enhanced or standard:

```
SVOS> secure-mode --help
Usage: secure-mode <enhanced | standard | status>

Set or retrieve the secure mode setting. Requires a zeroization to change modes.
SVOS>
...

SVOS> secure-mode enhanced
#####WARNING#####
This will set the switch into enhanced secure mode. Before
enhanced secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
#####WARNING#####

Continue (y/n)? y
reboot: Restarting system
...

...
```

```

SVOS> secure-mode standard
#####WARNING#####
This will set the switch into standard secure mode. Before
standard secure mode is enabled, the switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
#####WARNING#####

Continue (y/n)? y
reboot: Restarting system

...

...

SVOS> secure-mode standard
#####WARNING#####
Secure mode is already set to standard. Setting it again will
repeat the zeroization process. The switch must securely erase
all customer data and reset the switch to factory defaults.
This will initiate a reboot and render the switch unavailable
until the zeroization is complete.
This should take several minutes to one hour to complete.
#####WARNING#####

Continue (y/n)? y
reboot: Restarting system

...

...

SVOS> secure-mode status
enhanced secure mode is set.
SVOS>

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

sh

sh

Description

Launches a bash shell for support purposes. To quit bash, enter **exit**.

This command is not available if enhanced secure mode is set.

Example

Launching a bash shell:

```
SVOS> sh
switch:/cli/fs/home#
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

system serviceos password-prompt

```
system serviceos password-prompt
no system serviceos password-prompt
```

Description

Use this command to enable password authentication for ServiceOS. By default, the ServiceOS shell (accessible only from the local switch console port) requires no password to login as an admin use.

When this setting is enabled, the same password used to authenticate the admin user in the AOS-CX CLI or WeUI can be used to log in to the ServiceOS shell. If this setting is enabled, a forgotten admin user password cannot be reset using ServiceOS; if there are no other local or RADIUS/TACACS user accounts with administrator-level access, the switch must be zeroized by entering the **username zeroize** command at the ServiceOS login prompt to restore administrator access.

Example

Enabling password authentication for ServiceOS

```
switch(config)# system serviceos password-prompt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

umount

umount <DEVICE>

Description

Unmounts the SSD partitions mounted to the following locations: **/coredump**, **/logs**, **/nos**, **/selftest**, and unmounts the USB device mounted to **/mnt/usb**.

Parameter	Description
<DEVICE>	Specifies the device to be unmounted. Supported device options include all and usb .

Examples

Unmounting all devices:

```
SVOS> umount all
SVOS> umount usb
```

Unmounting a USB device:

```
SVOS> umount all
SVOS> umount usb
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (SVOS>)	Administrators or local user group members with execution rights for this command.

update

update {primary | secondary} <IMAGE>

Description

Verifies and installs a product image. The user can select the primary or secondary boot profile to update and the location of the file.

Parameter	Description
{primary secondary}	Selects either the primary or secondary image.
<IMAGE>	Specifies the image name.

Examples

Updating the software image using TFTP:



The OOBM port is disabled on first boot and must be enabled using the **ip** command.

```
SVOS> ip dhcp
SVOS> ip show
Interface   : Link Up
IP Address  : 192.0.2.22
Subnet Mask: 255.255.200.20
Gateway     : 10.0.24.1
SVOS> tftp -g -r XL.10.00.0001.swi -l image.swi 192.4.8.10
XL.10.00.0001.swi 100% |*****| 178M 0:00:00 ETA
SVOS> ls
image.swi
SVOS> update primary image.swi
Updating primary software image...
Verifying image...
Done
```

Update the software image using USB:



This example assumes that the user has preloaded a USB flash drive with the image to be updated. The image name on the flash drive is not important.

```
SVOS> mount usb
SVOS> ls /mnt/usb
image.swi
SVOS> update primary /mnt/usb/image.swi
Updating primary software image...
Verifying image...
Done
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (SVOS>)	Administrators or local user group members with execution rights for this command.

tftp

tftp {-b | -g | -l <LOCAL-FILE> | -p | -r <REMOTE-FILE>} host [<PORT>]

Description

Transfers files to and from a remote machine (TFTP a file).

Parameter	Description
{-b -g -l -p -r <REMOTE-FILE>}	Selects the options for transferring a file.
-b	Specifies the transfer blocks of size octets. The default blocksize is set to 1468, which can be overridden with the -b option.
-g	Specifies to get a file.
-l	Specifies a local file.
-p	Specifies to put a file in remote location.
-r <REMOTE-FILE>	Specifies a remote file.
<PORT>	Specifies the port for transfer. If no port option is specified, TFTP uses the standard UDP port 69 by default.

Example

Transferring files:

```
SVOS> tftp -b 65464 -g -r XL.10.00.0002.swi.swi 192.0.2.1
XL.10.00.0002 100% |*****| 178M 0:00:00 ETA
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	ServiceOS (SVOS>)	Administrators or local user group members with execution rights for this command.

version

version

Description

Displays the following build strings:

- Version.
- Build date.
- Build time.
- Build ID.
- SHA.

Example

Displaying version build strings:

```
SVOS> version
ServiceOS Information:
  Version:      GT.01.01.0001
  Build Date:   2017-07-19 14:52:31 PDT
  Build ID:     ServiceOS:GT.01.01.0001:461519208911:201707191452
  SHA:          46151920891195cdb2267ea6889a3c6cbc3d4193
SVOS>
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	ServiceOS (svos>)	Administrators or local user group members with execution rights for this command.

ACL application

ACLs can be applied as follows:

ACL type	IPv4+6	IPv4	IPv6	MAC
Direction	In	Out	Out	In
L2 interface (port)	Yes			Yes
L2 LAG	Yes			Yes
L3 interface (port)	Yes	Yes		Yes
L3 LAG	Yes	Yes		Yes
L3 interface (port) subinterface	Yes			Yes
L3 LAG subinterface	Yes			Yes
VLAN	Yes	Yes	Yes	Yes
Interface VLAN	Yes (routed)	Yes (routed)	Yes (routed)	
Management interface	Yes			
Control Plane (per VRF)	Yes			

HPE Aruba Networking 8325, 9300/9300S, 10000 Switch Series:

ACLs cannot match multicast packets on the routed in direction.

The following match criteria are not supported. If any of these match criteria are attempted to be configured, an error message will be displayed and the action will not be completed.



```
TCP flags CWR and ECE
TCP flags and TTL (hop limit) on IPv6 ACLs
TCP flags and fragment on outbound ACLs
Fragment on IPv6 VLAN ACLs
VLAN ID on VLAN ACLs
IPv4 AH on outbound ACLs
IPv6 AH on outbound ACLs
ESP on outbound ACLs
IPv4 AH on routed-outbound ACLs
IPv6 AH on routed-outbound ACLs
ESP on routed-outbound ACLs
```

To apply IPv4 and/or IPv6 ACLs to the management interface, apply them to the Control Plane on the management VRF.

access-list copy

```
access-list {ip|ipv6|mac} <ACL-NAME> copy <DESTINATION-ACL>
```

Description

Copies an IPv4, IPv6, or MAC ACL to a new destination ACL or overwrites an existing ACL.

Parameter	Description
{ip ipv6 mac}	Specifies the type of ACL.
<ACL-NAME>	Specifies the name of the ACL to be copied.
<DESTINATION-ACL>	Specifies the name of the destination ACL.

Examples

Copying *MY_IP_ACL* to *MY_IP_ACL2*:

```
switch(config)# access-list ip MY_IP_ACL copy MY_IP_ACL2
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      MY_IP_ACL
          1 permit
          any
          172.16.1.0/255.255.255.0
          udp
```



```

2 permit                                tcp
  172.16.2.0/255.255.0.0                > 1023
  any
3 permit                                tcp
  172.26.1.0/255.255.255.0
  any
  dscp: AF11
  ack
  syn
4 deny                                  any
  any
  any
  Hit-counts: enabled
-----
IPv4      MY_IP_ACL2
1 permit                                udp
  any
  172.16.1.0/255.255.255.0
2 permit                                tcp
  172.16.2.0/255.255.0.0                > 1023
  any
3 permit                                tcp
  172.26.1.0/255.255.255.0
  any
  dscp: AF11
  ack
  syn
4 deny                                  any
  any
  any
  Hit-counts: enabled

```

Copying MY_IPV6_ACL to MY_IPV6_ACL2:

```

switch(config)# access-list ipv6 MY_IPV6_ACL copy MY_IPV6_ACL2
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv6      MY_IPV6_ACL
1 permit                                udp
  any
  2001::1/64
2 Permit all TCP ephemeral ports
  permit                                tcp
  2001:2001::2:1          > 1023
  any
3 permit                                tcp
  2001:2011::1/64
  any
4 deny                                  any
  any
  any
  Hit-counts: enabled
-----

```

```
IPv6      MY_IPV6_ACL2
1 permit                                udp
  any
  2001::1/64
2 Permit all TCP ephemeral ports
  permit                                tcp
  2001:2001::2:1                        > 1023
  any
3 permit                                tcp
  2001:2011::1/64
  any
4 deny                                  any
  any
  any
Hit-counts: enabled
```

Copying MY_MAC_ACL to MY_MAC_ACL2:

```
switch(config)# access-list mac MY_MAC_ACL copy MY_MAC_ACL2
switch(config-acl-mac)# exit
```

```
switch(config)# do show access-list
```

Type	Name	Sequence	Comment	Action	EtherType
				Source MAC Address	Destination MAC Address
				Additional Parameters	

MAC	MY_MAC_ACL	1	permit	1122.3344.5566/ffff.ffff.0000	ipv6
			any		
		2	permit	aaaa.bbbb.cccc	any
				1111.2222.3333	
				QoS Priority Code Point: 4	
		3	Permit all vlan-1 tagged Appletalk traffic	permit	appletalk
			any		
			any		
			VLAN: 1		
		4	deny		any
			any		
			any		
			Hit-counts: enabled		

MAC	MY_MAC_ACL2	1	permit	1122.3344.5566/ffff.ffff.0000	ipv6
			any		
		2	permit	aaaa.bbbb.cccc	any
				1111.2222.3333	
				QoS Priority Code Point: 4	
		3	Permit all vlan-1 tagged Appletalk traffic	permit	appletalk
			any		
			any		
			VLAN: 1		
		4	deny		any

```

any
any
Hit-counts: enabled
Type Name
Sequence Comment
Action EtherType
Source MAC Address
Destination MAC Address
Additional Parameters
-----

```

```

MAC MY_MAC_ACL
1 permit 1122.3344.5566/ffff.ffff.0000 ipv6
any
2 permit aaaa.bbbb.cccc any
1111.2222.3333
QoS Priority Code Point: 4
3 Permit all vlan-1 tagged Appletalk traffic
permit appletalk
any
any
VLAN: 1
4 deny any
any
any
Hit-counts: enabled
-----

```

```

MAC MY_MAC_ACL2
1 permit 1122.3344.5566/ffff.ffff.0000 ipv6
any
2 permit aaaa.bbbb.cccc any
1111.2222.3333
QoS Priority Code Point: 4
3 Permit all vlan-1 tagged Appletalk traffic
permit appletalk
any
any
VLAN: 1
4 deny any
any
any
Hit-counts: enabled

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

access-list ip

Syntax to create an IPv4 ACL and enter its context. Plus syntax to remove an ACL:

```
access-list ip <ACL-NAME>
no access-list ip <ACL-NAME>
```

Syntax (within the ACL context) for creating or removing ACEs for protocols **ah**, **gre**, **esp**, **igmp**, **ospf**, **pim** (**ip** is available as an alias for **any**):

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{any|ip|ah|gre|esp|igmp|ospf|pim|<IP-PROTOCOL-NUM>}
{any|<SRC-IP-ADDRESS>[/(<PREFIX-LENGTH>|<SUBNET-MASK>)]|<ADDRESS-GROUP>}
{any|<DST-IP-ADDRESS>[/(<PREFIX-LENGTH>|<SUBNET-MASK>)]|<ADDRESS-GROUP>}
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>]
[count] [log]

no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for creating or removing ACEs for protocols **sctp**, **tcp**, **udp**:

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{sctp|tcp|udp}
{any|<SRC-IP-ADDRESS>[/(<PREFIX-LENGTH>|<SUBNET-MASK>)]|<ADDRESS-GROUP>}
[<eq|gt|lt> <PORT>|range <MIN-PORT> <MAX-PORT>|group <PORT-GROUP>]
{any|<DST-IP-ADDRESS>[/(<PREFIX-LENGTH>|<SUBNET-MASK>)]|<ADDRESS-GROUP>}
[<eq|gt|lt> <PORT>|range <MIN-PORT> <MAX-PORT>|group <PORT-GROUP>]
[urg] [ack] [psh] [rst] [syn] [fin] [established]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>]
[count] [log]

no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for creating or removing ACEs for protocol **icmp**:

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{icmp}
{any|<SRC-IP-ADDRESS>[/(<PREFIX-LENGTH>|<SUBNET-MASK>)]|<ADDRESS-GROUP>}
{any|<DST-IP-ADDRESS>[/(<PREFIX-LENGTH>|<SUBNET-MASK>)]|<ADDRESS-GROUP>}
[icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>]
[count] [log]

no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for ACE comments:

```
[<SEQUENCE-NUMBER>] comment <TEXT-STRING>

no <SEQUENCE-NUMBER> comment
```

Description

Creates an IPv4 Access Control List (ACL) comprised of one or more Access Control Entries (ACEs) ordered and prioritized by sequence number. The lowest sequence number is the highest prioritized ACE.

The **no** form of this command deletes the entire ACL, or deletes an ACE identified by sequence number, or deletes only the comment from the ACE identified by sequence number.

Parameter	Description
<code><ACL-NAME></code>	Specifies the name of this ACL.
<code><SEQUENCE-NUMBER></code>	Specifies a sequence number for the ACE. Range: 1 to 4294967295.
<code>{permit deny}</code>	Specifies whether to permit or deny traffic matching this ACE.
<code><IP-PROTOCOL-NUM></code>	Specifies the protocol as its Internet Protocol number. For example, 2 corresponds to the IGMP protocol. Range: 0 to 255.
<code>{any <SRC-IP-ADDRESS>[/{<PREFIX-LENGTH> <SUBNET-MASK>}] <ADDRESS-GROUP>}</code>	Specifies the source IPv4 address. ▪ any - specifies any source IPv4 address. ▪ <SRC-IP-ADDRESS> - specifies the source IPv4 host address. ◦ <PREFIX-LENGTH> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32. ◦ <SUBNET-MASK> - specifies the address bits to mask (dotted decimal notation). ▪ <ADDRESS-GROUP> - specifies an IPv4 address group defined with object-group ip address.
<code>{any <DST-IP-ADDRESS>[/{<PREFIX-LENGTH> <SUBNET-MASK>}] <ADDRESS-GROUP>}</code>	Specifies the destination IPv4 address. ▪ any - specifies any destination IPv4 address. ▪ <DST-IP-ADDRESS> - specifies the destination IPv4 host address. ◦ <PREFIX-LENGTH> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32. ◦ <SUBNET-MASK> - specifies the address bits to mask (dotted decimal notation). ▪ <ADDRESS-GROUP> - specifies an IPv4 address group that you defined earlier with object-group ip address.
<code>[{eq gt lt} <PORT> range <MIN-PORT> <MAX-PORT> group <PORT-GROUP>]</code>	Specifies the port, port range, or port group. Port numbers are in the range of 0 to 65535. ▪ eq <PORT> - specifies the Layer 4 port. ▪ gt <PORT> - specifies any Layer 4 port greater than the indicated port. ▪ lt <PORT> - specifies any Layer 4 port less than the indicated port. ▪ range <MIN-PORT> <MAX-PORT> - specifies the Layer 4 port range. ▪ group <PORT-GROUP> - specifies the Layer 4 port

Parameter	Description
	group that you defined earlier with <code>object-group port</code>. NOTE: Upon application of the ACL, ACEs with L4 port ranges may consume more than one hardware entry.
<code>urg</code>	Specifies matching on the TCP Flag: Urgent . (Applies only to the "in" (ingress) direction.)
<code>ack</code>	Specifies matching on the TCP Flag: Acknowledgment . (Applies only to the "in" (ingress) direction.)
<code>psh</code>	Specifies matching on the TCP Flag: Push buffered data to receiving application . (Applies only to the "in" (ingress) direction.)
<code>rst</code>	Specifies matching on the TCP Flag: Reset the connection . (Applies only to the "in" (ingress) direction.)
<code>syn</code>	Specifies matching on the TCP Flag: Synchronize sequence numbers . (Applies only to the "in" (ingress) direction.)
<code>fin</code>	Specifies matching on the TCP Flag: Finish connection . (Applies only to the "in" (ingress) direction.)
<code>established</code>	Specifies matching on the TCP Flag: Established connection. (Applies only to the "in" (ingress) direction.)
<code>[icmp-type {echo echo-reply <ICMP-TYPE-VALUE>}]</code>	Specifies the ICMP type. ▪ echo - specifies an ICMP echo request packet. ▪ echo-reply - specifies an ICMP echo reply packet. ▪ <ICMP-TYPE-VALUE> - specifies an ICMP type value. Range: 0 to 255.
<code>[icmp-code <ICMP-CODE-VALUE>]</code>	Specifies the ICMP code value. Range: 0 to 255.
<code>dscp DSCP-SPECIFIER></code>	Specifies the Differentiated Services Code Point (DSCP), either a numeric <DSCP-VALUE> (0 to 63) or one of these keywords: ▪ AF11 - DSCP 10 (Assured Forwarding Class 1, low drop probability) ▪ AF12 - DSCP 12 (Assured Forwarding Class 1, medium drop probability) ▪ AF13 - DSCP 14 (Assured Forwarding Class 1, high drop probability) ▪ AF21 - DSCP 18 (Assured Forwarding Class 2, low drop probability) ▪ AF22 - DSCP 20 (Assured Forwarding Class 2,

Parameter	Description
	medium drop probability) ▪ AF23 - DSCP 22 (Assured Forwarding Class 2, high drop probability) ▪ AF31 - DSCP 26 (Assured Forwarding Class 3, low drop probability) ▪ AF32 - DSCP 28 (Assured Forwarding Class 3, medium drop probability) ▪ AF33 - DSCP 30 (Assured Forwarding Class 3, high drop probability) ▪ AF41 - DSCP 34 (Assured Forwarding Class 4, low drop probability) ▪ AF42 - DSCP 36 (Assured Forwarding Class 4, medium drop probability) ▪ AF43 - DSCP 38 (Assured Forwarding Class 4, high drop probability) ▪ CS0 - DSCP 0 (Class Selector 0: Default) ▪ CS1 - DSCP 8 (Class Selector 1: Scavenger) ▪ CS2 - DSCP 16 (Class Selector 2: OAM) ▪ CS3 - DSCP 24 (Class Selector 3: Signaling) ▪ CS4 - DSCP 32 (Class Selector 4: Real time) ▪ CS5 - DSCP 40 (Class Selector 5: Broadcast video) ▪ CS6 - DSCP 48 (Class Selector 6: Network control) ▪ CS7 - DSCP 56 (Class Selector 7) ▪ EF - DSCP 46 (Expedited Forwarding)
<code>ecn <ECN-VALUE></code>	Specifies an Explicit Congestion Notification value. Range: 0 to 3.
<code>ip-precedence <IP-PRECEDENCE-VALUE></code>	Specifies an IP precedence value. Range: 0 to 7.
<code>tos <TOS-VALUE></code>	Specifies the Type of Service value. Range: 0 to 31.
<code>fragment</code>	Specifies a fragment packet.
<code>vlan <VLAN-ID></code>	Specifies VLAN tag to match on. 802.1Q VLAN ID. NOTE: This parameter cannot be used in any ACL that will be applied to a VLAN.
<code>ttl <TTL-VALUE></code>	Specifies a time-to-live (hop limit) value. Range: 0 to 255.
<code>count</code>	Keeps the hit counts of the number of packets matching this ACE.
<code>log</code>	Keeps a log of the number of packets matching this ACE. Works with <code>deny</code> actions but not with <code>permit</code> actions. Works with ACLs applied on ingress, or Control Plane, but not with ACLs applied on egress.

Parameter	Description
[<SEQUENCE-NUMBER>] comment <TEXT-STRING>	Adds a comment to an ACE. The no form removes only the comment from the ACE.

Usage

- If the **<IP-PROTOCOL-NUM>** parameter is used instead of a protocol name, ensure that any needed ACE-definition parameters specific to the selected protocol are also provided.
- When using multiple ACL types (IPv4, IPv6, or MAC) with logging on the same interface, the first packet that matches an ACE with **log** option is logged. Until the log-timer wait-period is over, any packets matching other ACL types do not create a log. At the end of the wait-period, the switch creates a summary log for all the ACLs that were matched, regardless of type.

Examples

Creating an IPv4 ACL with four entries:

```
switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# 10 permit udp any 172.16.1.0/24
switch(config-acl-ip)# 20 permit tcp 172.16.2.0/16 gt 1023 any
switch(config-acl-ip)# 30 permit tcp 172.26.1.0/24 any syn ack dscp 10
switch(config-acl-ip)# 40 deny any any any count
switch(config-acl-ip)# exit

switch(config)# show access-list
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      MY_IP_ACL
10 permit                                udp
   any
   172.16.1.0/255.255.255.0
20 permit                                tcp
   172.16.2.0/255.255.0.0
   any
   > 1023
30 permit                                tcp
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn
40 deny                                    any
   any
   any
Hit-counts: enabled
```

Adding a comment to an existing IPv4 ACE:

```
switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# 20 comment Permit all TCP ephemeral ports
switch(config-acl-ip)# exit
```



```

switch(config)# show access-list
Type          Name
Sequence      Comment
              Action
              Source IP Address
              Destination IP Address
              Additional Parameters
-----
IPv4          MY_IP_ACL
10 permit
   any
   172.16.1.0/255.255.255.0
20 Permit all TCP ephemeral ports
   permit
   172.16.2.0/255.255.0.0
   any
30 permit
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn
40 deny
   any
   any
Hit-counts: enabled
L3 Protocol
Source L4 Port(s)
Destination L4 Port(s)
udp
tcp
tcp
any

```

Removing a comment from an existing IPv4 ACE:

```

switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# no 20 comment
switch(config-acl-ip)# exit

switch(config)# show access-list
Type          Name
Sequence      Comment
              Action
              Source IP Address
              Destination IP Address
              Additional Parameters
-----
IPv4          MY_IP_ACL
10 permit
   any
   172.16.1.0/255.255.255.0
20 permit
   172.16.2.0/255.255.0.0
   any
30 permit
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn
40 deny
   any
   any
Hit-counts: enabled
L3 Protocol
Source L4 Port(s)
Destination L4 Port(s)
udp
tcp
tcp
any

```

Adding an ACE (insert line 25) to an existing IPv4 ACL:

```

switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# 25 permit icmp 172.16.2.0/16 any
switch(config-acl-ip)# exit

switch(config)# show access-list
Type      Name
Sequence Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      MY_IP_ACL
10 permit
   any
   172.16.1.0/255.255.255.0
20 permit
   172.16.2.0/255.255.0.0
   any
25 permit
   172.16.2.0/255.255.0.0 any
30 permit
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn
40 deny
   any
   any
   Hit-counts: enabled

```

Replacing an ACE in an existing IPv4 ACL:

```

switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# 25 permit icmp 172.17.1.0/16 any
switch(config-acl-ip)# exit

switch(config)# show access-list
Type      Name
Sequence Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      MY_IP_ACL
10 permit
   any
   172.16.1.0/255.255.255.0
20 permit
   172.16.2.0/255.255.0.0
   any
25 permit
   172.17.1.0/255.255.0.0
30 permit
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn

```

```

40 deny
any
any
Hit-counts: enabled
Type      Name
Sequence Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv4      MY_IP_ACL
10 permit
any
172.16.1.0/255.255.255.0
20 permit
172.16.2.0/255.255.0.0
any
25 permit
172.17.1.0/255.255.0.0
30 permit
172.26.1.0/255.255.255.0
any
dscp: AF11
ack
syn
40 deny
any
any
Hit-counts: enabled

```

Removing an ACE from an IPv4 ACL:

```

switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# no 25
switch(config-acl-ip)# exit

switch(config)# show access-list
Type      Name
Sequence Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv4      MY_IP_ACL
10 permit
any
172.16.1.0/255.255.255.0
20 permit
172.16.2.0/255.255.0.0
any
30 permit
172.26.1.0/255.255.255.0
any
dscp: AF11
ack
syn
40 deny
any
any

```

```

Hit-counts: enabled
Type      Name
Sequence Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv4      MY_IP_ACL
10 permit                udp
   any
   172.16.1.0/255.255.255.0
20 permit                tcp
   172.16.2.0/255.255.0.0    > 1023
   any
30 permit                tcp
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn
40 deny                  any
   any
   any
Hit-counts: enabled

```

Copy an IPv4 ACL:

```

switch(config)# access-list ip MY_IP_ACL copy MY_IP_ACL2
switch(config)# show access-list
Type      Name
Sequence Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv4      MY_IP_ACL
10 permit                udp
   any
   172.16.1.0/255.255.255.0
20 permit                tcp
   172.16.2.0/255.255.0.0    > 1023
   any
30 permit                tcp
   172.26.1.0/255.255.255.0
   any
   dscp: AF11
   ack
   syn
40 deny                  any
   any
   any
Hit-counts: enabled
-----
IPv4      MY_IP_ACL2
10

```

```

        permit
        any
        172.16.1.0/255.255.255.0
20    permit
        172.16.2.0/255.255.0.0
        any
30    permit
        172.26.1.0/255.255.255.0
        any
        dscp: AF11
        ack
        syn
40    deny
        any
        any
        any
Hit-counts: enabled switch(config)# access-list ip MY_IP_ACL copy MY_
IP_ACL2

```

switch(config)# **show access-list**

Type	Sequence	Name	Comment	Action	L3 Protocol	Source IP Address	Source L4 Port(s)	Destination IP Address	Destination L4 Port(s)	Additional Parameters
IPv4		MY_IP_ACL								
	10			permit	udp	any				
				any		172.16.1.0/255.255.255.0				
	20			permit	tcp	172.16.2.0/255.255.0.0	> 1023			
				any						
	30			permit	tcp	172.26.1.0/255.255.255.0				
				any						
				dscp: AF11						
				ack						
				syn						
	40			deny	any					
				any						
				any						
				Hit-counts: enabled						
IPv4		MY_IP_ACL2								
	10			permit	udp	any				
				any		172.16.1.0/255.255.255.0				
	20			permit	tcp	172.16.2.0/255.255.0.0	> 1023			
				any						
	30			permit	tcp					

```

172.26.1.0/255.255.255.0
any
dscp: AF11
ack
syn
40
deny
any
any
Hit-counts: enabled
any

```

Removing an IPv4 ACL:

```

switch(config)# no access-list ip MY_IP_ACL

switch(config)# show access-list
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      MY_IP_ACL2
1 permit
  any
  172.16.1.0/255.255.255.0
2 permit
  172.16.2.0/255.255.0.0
  any
3 permit
  172.26.1.0/255.255.255.0
  any
  dscp: AF11
  ack
  syn
4 deny
  any
  any
Hit-counts: enabled
          L3 Protocol
          Source L4 Port(s)
          Destination L4 Port(s)
          udp
          tcp
          > 1023
          tcp
          any

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.12	Allow ACLs applied to the Control Plane to be logged.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config The access-list ip <ACL-NAME> command takes you into the named ACL context where you enter the ACEs.	Administrators or local user group members with execution rights for this command.

access-list ipv6

Syntax to create an IPv6 ACL and enter its context. Plus syntax to remove an ACL:

```
access-list ipv6 <ACL-NAME>
no access-list ipv6 <ACL-NAME>
```

Syntax (within the ACL context) for creating or removing ACEs for protocols **ah**, **gre**, **esp**, **ospf**, **pim** (**ipv6** is available as an alias for **any**):

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{any|ipv6|ah|gre|esp|ospf|pim|<IP-PROTOCOL-NUM>}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>]|<ADDRESS-GROUP>}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]|<ADDRESS-GROUP>}
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count] [log]
```

```
no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for creating or removing ACEs for protocols **sctp**, **tcp**, **udp**:

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{sctp|tcp|udp}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>]|<ADDRESS-GROUP>}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>|group <PORT-GROUP>]
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]|<ADDRESS-GROUP>}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>|group <PORT-GROUP>]
[urg] [ack] [psh] [rst] [syn] [fin] [established]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count] [log]
```

```
no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for creating or removing ACEs for protocol **icmpv6**:

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{icmpv6}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>]|<ADDRESS-GROUP>}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]|<ADDRESS-GROUP>}
[icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count] [log]
```

```
no <SEQUENCE-NUMBER>
```

Syntax (within the ACL context) for ACE comments:

```
[<SEQUENCE-NUMBER>] comment <TEXT-STRING>
```

```
no <SEQUENCE-NUMBER> comment
```

Description

Creates an IPv6 Access Control List (ACL). The ACL is made of one or more Access Control Entries (ACEs) ordered and prioritized by sequence number. The lowest sequence number is the highest prioritized ACE.

The **no** form of this command deletes the entire ACL, or deletes an ACE identified by sequence number, or deletes only the comment from the ACE identified by sequence number.

Parameter	Description
<code><ACL-NAME></code>	Specifies the name of this ACL.
<code><SEQUENCE-NUMBER></code>	Specifies a sequence number for the ACE. Range: 1 to 4294967295.
<code>{permit deny}</code>	Specifies whether to permit or deny traffic matching this ACE.
<code><IP-PROTOCOL-NUM></code>	Specifies the protocol as its Internet Protocol number. For example, 2 corresponds to the IGMP protocol. Range: 0 to 255.
<code>{any <SRC-IP-ADDRESS>[/<PREFIX-LENGTH>] <ADDRESS-GROUP>}</code>	Specifies the source IPv6 address. ▪ any - specifies any source IPv6 address. ▪ <SRC-IP-ADDRESS> - specifies the source IPv6 host address. ◦ <PREFIX-LENGTH> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 128. ▪ <ADDRESS-GROUP> - specifies an IPv6 address group that you defined earlier with object-group ipv6 address.
<code>{any <DST-IP-ADDRESS>[/<PREFIX-LENGTH>] <ADDRESS-GROUP>}</code>	Specifies the destination IPv6 address. ▪ any - specifies any destination IPv6 address. ▪ <DST-IP-ADDRESS> - specifies the destination IPv6 host address. ◦ <PREFIX-LENGTH> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 128. ▪ <ADDRESS-GROUP> - specifies an IPv6 address group that you defined earlier with object-group ipv6 address.
<code>[{eq gt lt} <PORT> range <MIN-PORT><MAX-PORT> group <PORT-GROUP>]</code>	Specifies the port, port range, or port group. Port numbers are in the range of 0 to 65535. ▪ eq <PORT> - specifies the Layer 4 port. ▪ gt <PORT> - specifies any Layer 4 port greater than the indicated port. ▪ lt <PORT> - specifies any Layer 4 port less than the indicated port. ▪ range <MIN-PORT> <MAX-PORT> - specifies the Layer 4 port range. ▪ group <PORT-GROUP> - specifies the Layer 4 port group that you defined earlier with object-group port.

Parameter	Description
	NOTE: Upon application of the ACL, ACEs with L4 port ranges may consume more than one hardware entry.
<code>urg, ack, psh, rst, syn, fin, established</code>	These TCP flag-matching parameters are not supported.
<code>[icmp-type {echo echo-reply <ICMP-TYPE-VALUE>}]</code>	Specifies the ICMP type. ▪ echo - specifies an ICMP echo request packet. ▪ echo-reply - specifies an ICMP echo reply packet. ▪ <ICMP-TYPE-VALUE> - specifies an ICMP type value. Range: 0 to 255.
<code>[icmp-code <ICMP-CODE-VALUE>]</code>	Specifies the ICMP code value. Range: 0 to 255.
<code>dscp DSCP-SPECIFIER></code>	Specifies the Differentiated Services Code Point (DSCP), either a numeric <DSCP-VALUE> (0 to 63) or one of these keywords: ▪ AF11 - DSCP 10 (Assured Forwarding Class 1, low drop probability) ▪ AF12 - DSCP 12 (Assured Forwarding Class 1, medium drop probability) ▪ AF13 - DSCP 14 (Assured Forwarding Class 1, high drop probability) ▪ AF21 - DSCP 18 (Assured Forwarding Class 2, low drop probability) ▪ AF22 - DSCP 20 (Assured Forwarding Class 2, medium drop probability) ▪ AF23 - DSCP 22 (Assured Forwarding Class 2, high drop probability) ▪ AF31 - DSCP 26 (Assured Forwarding Class 3, low drop probability) ▪ AF32 - DSCP 28 (Assured Forwarding Class 3, medium drop probability) ▪ AF33 - DSCP 30 (Assured Forwarding Class 3, high drop probability) ▪ AF41 - DSCP 34 (Assured Forwarding Class 4, low drop probability) ▪ AF42 - DSCP 36 (Assured Forwarding Class 4, medium drop probability) ▪ AF43 - DSCP 38 (Assured Forwarding Class 4, high drop probability) ▪ CS0 - DSCP 0 (Class Selector 0: Default) ▪ CS1 - DSCP 8 (Class Selector 1: Scavenger) ▪ CS2 - DSCP 16 (Class Selector 2: OAM) ▪ CS3 - DSCP 24 (Class Selector 3: Signaling) ▪ CS4 - DSCP 32 (Class Selector 4: Real time) ▪ CS5 - DSCP 40 (Class Selector 5: Broadcast video) ▪ CS6 - DSCP 48 (Class Selector 6: Network control) ▪ CS7 - DSCP 56 (Class Selector 7)

Parameter	Description
	▪ EF - DSCP 46 (Expedited Forwarding)
ecn <ECN-VALUE>	Specifies an Explicit Congestion Notification value. Range: 0- 3.
ip-precedence <IP-PRECEDENCE-VALUE>	Specifies an IP precedence value. Range: 0-7.
tos <TOS-VALUE>	Specifies the Type of Service value. Range: 0-31.
fragment	Not supported.
vlan <VLAN-ID>	Not supported.
ttl <TTL-VALUE>	Not supported.
count	Keeps the hit counts of the number of packets matching this ACE.
log	Keeps a log of the number of packets matching this ACE. Works with <code>deny</code> actions but not with <code>permit</code> actions. Works with ACLs applied on ingress, or Control Plane, but not with ACLs applied on egress.
[<SEQUENCE-NUMBER>] comment <TEXT-STRING>	Adds a comment to an ACE. The no form removes only the comment from the ACE.

Usage

- If the **<IP-PROTOCOL-NUM>** parameter is used instead of a protocol name, ensure that any needed ACE-definition parameters specific to the selected protocol are also provided.
- When using multiple ACL types (IPv4, IPv6, or MAC) with logging on the same interface, the first packet that matches an ACE with `log` option is logged. Until the log-timer wait-period is over, any packets matching other ACL types do not create a log. At the end of the wait-period, the switch creates a summary log all the ACLs that were matched, regardless of type.

Examples

Creating an IPv6 ACL with four entries:

```
switch(config)# access-list ipv6 MY_IPV6_ACL
switch(config-acl-ipv6)# 10 permit udp any 2001::1/64
switch(config-acl-ipv6)# 20 permit tcp 2001:2001::2:1/128 gt 1023 any
switch(config-acl-ipv6)# 30 permit tcp 2001:2011::1/64 any
switch(config-acl-ipv6)# 40 deny any any any count
switch(config-acl-ipv6)# exit

switch(config)# do show access-list
Type      Name
Sequence Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv6      MY_IPV6_ACL
```

```

10 permit                                udp
   any
   2001::1/64
20 permit                                tcp
   2001:2001::2:1                        > 1023
   any
30 permit                                tcp
   2001:2011::1/64
   any
40 deny                                  any
   any
   any
Hit-counts: enabled

```

Adding a comment to an existing IPv6 ACE:

```

switch(config)# access-list ipv6 MY_IPV6_ACL
switch(config-acl-ipv6)# 20 comment Permit all TCP ephemeral ports
switch(config-acl-ipv6)# exit

switch(config)# do show access-list
Type      Name
Sequence Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters  Destination L4 Port(s)
-----
IPv6      MY_IPV6_ACL
10 permit                                udp
   any
   2001::1/64
20 Permit all TCP ephemeral ports
   permit                                tcp
   2001:2001::2:1                        > 1023
   any
30 permit                                tcp
   2001:2011::1/64
   any
40 deny                                  any
   any
   any
Hit-counts: enabled

```

Removing a comment from an existing IPv6 ACE:

```

switch(config)# access-list ipv6 MY_IPV6_ACL
switch(config-acl-ipv6)# no 20 comment
switch(config-acl-ipv6)# exit

switch(config)# do show access-list
Type      Name
Sequence Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters  Destination L4 Port(s)
-----
IPv6      MY_IPV6_ACL

```

```

10 permit                                udp
   any
   2001::1/64
20 permit                                tcp
   2001:2001::2:1                        > 1023
   any
30 permit                                tcp
   2001:2011::1/64
   any
40 deny                                  any
   any
   any
Hit-counts: enabled

```

Adding an ACE to an existing IPv6 ACL:

```

switch(config)# access-list ipv6 MY_IPV6_ACL
switch(config-acl-ipv6)# 25 permit icmpv6 2001::1/64 any
switch(config-acl-ipv6)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv6      MY_IPV6_ACL
10 permit                                udp
   any
   2001::1/64
20 permit                                tcp
   2001:2001::2:1                        > 1023
   any
25 permit                                icmpv6
   2001::1/64
   any
30 permit                                tcp
   2001:2011::1/64
   any
40 deny                                  any
   any
   any
Hit-counts: enabled

```

Replacing an ACE in an existing IPv6 ACL:

```

switch(config)# access-list ipv6 MY_IPV6_ACL
switch(config-acl-ipv6)# 25 permit icmpv6 2001::2:1/64 any
switch(config-acl-ipv6)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)

```

```

-----
IPv6      MY_IPV6_ACL
10 permit any                udp
    2001::1/64
20 permit any                tcp
    2001:2001::2:1          > 1023
25 permit any                icmpv6
    2001::2:1/64
30 permit any                tcp
    2001:2011::1/64
40 deny any                  any
    any
    any
Hit-counts: enabled

Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv6      MY_IPV6_ACL
10 permit any                udp
    2001::1/64
20 permit any                tcp
    2001:2001::2:1          > 1023
25 permit any                icmpv6
    2001::2:1/64
30 permit any                tcp
    2001:2011::1/64
40 deny any                  any
    any
    any
Hit-counts: enabled

```

Removing an ACE from an IPv6 ACL:

```

switch(config)# access-list ipv6 MY_IPV6_ACL
switch(config-acl-ipv6)# no 25
switch(config-acl-ipv6)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv6      MY_IPV6_ACL
10 permit any                udp

```

```

    2001::1/64
20 permit                                tcp
    2001:2001::2:1                        > 1023
    any
30 permit                                tcp
    2001:2011::1/64
    any
40 deny                                  any
    any
    any
Hit-counts: enabled

Type      Name
Sequence  Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv6      MY_IPV6_ACL
10 permit                                udp
    any
    2001::1/64
20 permit                                tcp
    2001:2001::2:1                        > 1023
    any
30 permit                                tcp
    2001:2011::1/64
    any
40 deny                                  any
    any
    any
Hit-counts: enabled

```

Removing an IPv6 ACL:

```

switch(config)# no access-list ipv6 MY_IPV6_ACL

switch(config)# do show access-list
Type      Name
Sequence  Comment
Action
Source IP Address      L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters   Destination L4 Port(s)
-----
IPv6      MY_IPV6_ACL2
1 permit                                udp
    any
    2001::1/64
2 Permit all TCP ephemeral ports
  permit                                tcp
    2001:2001::2:1                        > 1023
    any
3 permit                                tcp
    2001:2011::1/64
    any
4 deny                                  any
    any
    any
Hit-counts: enabled

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.12	Allow ACLs applied to the Control Plane to be logged.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code> The access-list ipv6 <ACL-NAME> command takes you into the named ACL context where you enter the ACEs.	Administrators or local user group members with execution rights for this command.

access-list log-timer

```
access-list log-timer {default|<INTERVAL>}
```

Description

Sets the log timer interval for all ACEs that have the **log** parameter configured.

Parameter	Description
<code>default</code>	Resets the log timer to its default 300 seconds.
<code><INTERVAL></code>	Specifies the log timer interval in seconds. Range: 5 to 300.

Usage

- ACL logging keeps a log of the number of packets matching this ACE. Works with `deny` actions but not with `permit` actions. Works with ACLs applied on ingress, or Control Plane, but not with ACLs applied on egress.
- The first packet that matches an ACE with the **log** parameter within an ACL log timer window (configured with the **access-list log-timer** command) has its header contents extracted and sent to the configured logging destination, such as the console and syslog server. Each time the ACL log timer expires, a summary of all ACEs with **log** configured are sent to the logging destination. This capability allows throttling of logging ACL hits.
- If no further log messages are generated in the wait-period, the switch suspends the timer and resets itself to log as soon as a new match occurs.
- When using multiple ACL types (IPv4, IPv6, or MAC) with logging on the same interface, the first packet that matches an ACE with the `log` option is logged. Any packets, matching other ACL types, do

not create a log until the log-timer wait-period is over. At the end of the wait-period, a summary log is made of all the ACLs that were matched, regardless of type.

- You may see a minor discrepancy between the ACL logging statistics and the hit counts statistics due to the time required to record the log message.

Examples



Although these examples use debug logging, you can alternatively use event logging.

Enabling debug logging for the ACL logging module:

```
switch# debug acl log severity info
switch# show debug
-----
module sub_module severity vlan port ip mac instance vrf
-----
acl acl_log info -----
```

Setting the debug destination to console with the minimum security level of info:

```
switch# debug destination console severity info
switch# show debug destination
-----
show debug destination
-----
CONSOLE:info
```

Setting the access list log-timer to 30 seconds:

```
switch(config)# access-list log-timer 30
switch(config)# do show access-list log-timer
ACL log timer length (frequency): 30 seconds
```

Creating an IPv4 ACL with one entry with the log parameter:

```
switch(config)# access-list ip MY_IP_ACL
switch(config-acl-ip)# deny icmp 1.1.1.1 1.1.1.2 log
switch(config-acl-ip)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      MY_IP_ACL
10 deny
1.1.1.1
1.1.1.2
Logging: enabled
Hit-counts: enabled
          L3 Protocol
          Source L4 Port(s)
          Destination L4 Port(s)
```

Enabling interface 1/1/1 and applying the ACL:


```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# apply access-list ip MY_IP_ACL in
switch(config-if)# do show running-config interface 1/1/1
interface 1/1/1
  no shutdown
  apply access-list ip MY_IP_ACL in
  no routing
  vlan access 1
  exit
```

Sending packets that will match the ACE and observe the ACL logging message on the console:

```
2017-10-10T20:13:36.044+00:00 ops-switchd[875]: debug|LOG_INFO|AMM|1/5|ACL|ACL_
LOG|
List MY_IP_ACL, seq# 10 denied icmp 1.1.1.1 -> 1.1.1.2 type 8 code 0,
on vlan 1, port 1/1/1, direction in
```

When the access list log-timer expires, the summary message is printed on the console. The number 30 is the number of packets received during the last access list log-timer window.

```
2017-10-10T20:14:06.051+00:00 ops-switchd[875]: debug|LOG_INFO|AMM|1/5|ACL|ACL_
LOG|
MY_IP_ACL on 1/1/1 (in): 30 10 deny icmp 1.1.1.1 1.1.1.2 log count
```

Resetting the ACL log timer to the default value:

```
switch(config)# access-list log-timer default
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.12	Allow ACLs applied to the Control Plane to be logged.
10.09	<INTERVAL> parameter range changed to 5 to 300 . Was 30 to 300.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

access-list mac

```
access-list mac <ACL-NAME>
no access-list mac <ACL-NAME>
```

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{any|<SRC-MAC-ADDRESS>[/<ETHERNET-MASK>]}}
{any|<DST-MAC-ADDRESS>[/<ETHERNET-MASK>]}}
{any|arp|appletalk|arp|fcoe|fcoe-init|ip|ipv6|
    ipx-arpa|ipx-non-arpa|is-is|lldp|mpls-multicast|mpls-unicast|q-in-q|
    rbridge|trill|wake-on-lan|<NUMERIC-ETHERTYPE>}}
[pcp <PCP-VALUE>] [vlan <VLAN-ID>] [count] [log]
no <SEQUENCE-NUMBER>
```

```
[<SEQUENCE-NUMBER>] comment <TEXT-STRING>
no <SEQUENCE-NUMBER> comment
```

Description

Creates a MAC Access Control List (ACL). The ACL is made of one or more Access Control Entries (ACEs) ordered and prioritized by sequence numbers. The lowest sequence number is the highest prioritized ACE.

The **no** form of this command deletes the entire ACL, or deletes an ACE identified by sequence number, or deletes only the comment from the ACE identified by sequence number.

Parameter	Description
<ACL-NAME>	Specifies the name of this ACL.
<SEQUENCE-NUMBER>	Specifies a sequence number for the ACE. Range: 1 to 4294967295.
{permit deny}	Specifies whether to permit or deny traffic matching this ACE.
comment	Specifies storing the remaining entered text as an ACE comment.
{any <SRC-MAC-ADDRESS>[/<ETHERNET-MASK>]}}	Specifies the source host MAC address (xxxx.xxxx.xxxx), OUI, or the keyword <i>any</i> . You can optionally include the following: <ETHERNET-MASK> - The address bits to mask (xxxx.xxxx.xxxx).
{any <DST-MAC-ADDRESS>[/<ETHERNET-MASK>]}}	Specifies the destination host MAC address (xxxx.xxxx.xxxx), OUI, or the keyword <i>any</i> . You can optionally include the following: <ETHERNET-MASK> - The address bits to mask (xxxx.xxxx.xxxx).
{any arp appletalk ... wake-on-lan <NUMERIC-ETHERTYPE>}	Specifies the protocol encapsulated in the Ethernet frame. The encapsulated protocol is identified by the EtherType Ethernet field. The EtherType is specified in one of the following three ways: - any - any EtherType. <NUMERIC-ETHERTYPE> - the numerical EtherType protocol number. Range: 0x600 to 0xffff. - One of these EtherType protocol name keywords: - arp - appletalk

Parameter	Description
	- arp - fcoe - fcoe-init - ip - ipv6 - ipx-arpa - ipx-non-arpa - is-is - lldp - mpls-multicast - mpls-unicast - q-in-q - rbridge - trill - wake-on-lan
pcp <PCP-VALUE>	Specifies 802.1Q QoS Priority Code Point value. Range: 0 to 7.
vlan <VID>	Specifies a VLAN ID. The VLAN ID must exist. NOTE: This parameter cannot be used in any ACL that will be applied to a VLAN.
count	Keeps the hit counts of the number of packets matching this ACE.
log	Keeps a log of the number of packets matching this ACE. Works with deny actions but not with permit actions. Works with ACLs applied on ingress but not with ACLs applied on egress.

Usage

When using multiple ACL types (IPv4, IPv6, or MAC) with logging on the same interface, the first packet that matches an ACE with log option is logged. Until the log-timer wait-period is over, any packets matching other ACL types do not create a log. At the end of the wait-period, the switch creates a summary log all the ACLs that were matched, regardless of type.

Examples

Creating a MAC ACL with four entries:

```
switch(config)# access-list mac MY_MAC_ACL
switch(config-acl-ip)# 10 permit 1122.3344.5566/ffff.ffff.0000 any ipv6
switch(config-acl-ip)# 20 permit aaaa.bbbb.cccc 1111.2222.3333 any pcp 4
switch(config-acl-ip)# 30 permit any any appletalk vlan 40
switch(config-acl-ip)# 40 deny any any any count
switch(config-acl-ip)# exit

switch(config)# do show access-list
```

Type	Name	
Sequence	Comment	
	Action	EtherType
	Source MAC Address	
	Destination MAC Address	
	Additional Parameters	
MAC	MY_MAC_ACL	
10	permit 1122.3344.5566/ffff.ffff.0000 any	ipv6
20	permit aaaa.bbbb.cccc 1111.2222.3333 QoS Priority Code Point: 4	any
30	permit any any VLAN: 40	appletalk
40	deny any any Hit-counts: enabled	any

Adding a comment to an existing MAC ACE:

```
switch(config)# access-list mac MY_MAC_ACL
switch(config-acl-ip)# 30 comment Permit all vlan-40 tagged Appletalk traffic
switch(config-acl-ip)# exit
```

```
switch(config)# do show access-list
```

Type	Name		
Sequence	Comment		
	Action		EtherType
	Source MAC Address		
	Destination MAC Address		
	Additional Parameters		
MAC	MY_MAC_ACL		
10	permit		ipv6
	1122.3344.5566/ffff.ffff.0000		
	any		
20	permit		any
	aaaa.bbbb.cccc		
	1111.2222.3333		
	QoS Priority Code Point: 4		
30	Permit all vlan-40 tagged Appletalk traffic		
	permit		appletalk
	any		
	any		
	VLAN: 40		
40	deny		any
	any		
	any		
	Hit-counts: enabled		

Removing a comment from an existing MAC ACE:

```

switch(config)# access-list mac MY_MAC_ACL
switch(config-acl-mac)# no 30 comment
switch(config-acl-mac)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source MAC Address
          Destination MAC Address
          Additional Parameters
-----
MAC       MY_MAC_ACL
10 permit 1122.3344.5566/ffff.ffff.0000      ipv6
   any
20 permit aaaa.bbbb.cccc                      any
   1111.2222.3333
   QoS Priority Code Point: 4
30 permit any                                appletalk
   any
   any
   VLAN: 1
40 deny   any                                any
   any
   any
Hit-counts: enabled

```

Adding an ACE to an existing MAC ACL:

```

switch(config)# access-list mac MY_MAC_ACL
switch(config-acl-ip)# 35 permit any aabb.cc11.1234 0xffee
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source MAC Address
          Destination MAC Address
          Additional Parameters
-----
MAC       MY_MAC_ACL
10 permit 1122.3344.5566/ffff.ffff.0000      ipv6
   any
20 permit aaaa.bbbb.cccc                      any
   1111.2222.3333
   QoS Priority Code Point: 4
30 permit any                                appletalk
   any
   any
   VLAN: 1
35 permit any                                0xffee
   aabb.cc11.1234
40 deny   any                                any
   any
   any

```

```
Hit-counts: enabled
```

Replacing an ACE in an existing MAC ACL:

```
switch(config)# access-list mac MY_MAC_ACL
switch(config-acl-ip)# 35 permit any aabb.cc11.1234 0xeeee
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source MAC Address
          Destination MAC Address
          Additional Parameters
-----
MAC       MY_MAC_ACL
10 permit 1122.3344.5566/ffff.ffff.0000      ipv6
   any
20 permit aaaa.bbbb.cccc                        any
   1111.2222.3333
   QoS Priority Code Point: 4
30 permit any                                appletalk
   any
   VLAN: 1
35 permit any                                0xeeee
   aabb.cc11.1234
40 deny   any                                any
   any
Hit-counts: enabled
```

Removing an ACE from an MAC ACL:

```
switch(config)# access-list mac MY_MAC_ACL
switch(config-acl-ip)# no 35
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source MAC Address
          Destination MAC Address
          Additional Parameters
-----
MAC       MY_MAC_ACL
10 permit 1122.3344.5566/ffff.ffff.0000      ipv6
   any
20 permit aaaa.bbbb.cccc                        any
   1111.2222.3333
   QoS Priority Code Point: 4
30 permit any                                appletalk
```

```

any
any
VLAN: 1
40 deny any
any
any
Hit-counts: enabled

```

Removing a MAC ACL:

```

switch(config)# no access-list mac MY_MAC_ACL

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source MAC Address
          Destination MAC Address
          Additional Parameters
-----
MAC       MY_MAC_ACL2
1 permit 1122.3344.5566/ffff.ffff.0000 ipv6
any
2 permit aaaa.bbbb.cccc any
1111.2222.3333
QoS Priority Code Point: 4
3 Permit all vlan-40 tagged Appletalk traffic
permit appletalk
any
any
VLAN: 1
4 deny any
any
any
Hit-counts: enabled

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config The <code>access-list mac <ACL-NAME></code> command takes you into the named	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
	ACL context where you enter the ACEs.	

access-list resequence

`access-list {ip|ipv6|mac} <ACL-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>`

Description

Resequences the ACE sequence numbers in an ACL.

Parameter	Description
{ip ipv6 mac}	Specifies the ACL type.
<ACL-NAME>	Specifies the ACL name.
<STARTING-SEQUENCE-NUMBER>	Specifies the starting sequence number.
<INCREMENT>	Specifies the sequence number increment.

Examples

Resequencing an IPv4 ACL to start at 1 with an increment of 1:

```
switch(config)# access-list ip MY_IP_ACL resequence 1 1
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action          L3 Protocol
          Source IP Address Source L4 Port(s)
          Destination IP Address Destination L4 Port(s)
          Additional Parameters
-----
IPv4      MY_IP_ACL
1 permit          udp
  any
  172.16.1.0/255.255.255.0
2 permit          tcp
  172.16.2.0/255.255.0.0    > 1023
  any
3 permit          tcp
  172.26.1.0/255.255.255.0
  any
  dscp: AF11
  ack
  syn
4 deny          any
  any
  any
Hit-counts: enabled
```

Resequencing an IPv6 ACL to start at 1 with an increment of 1:


```

switch(config)# access-list ipv6 MY_IPV6_ACL resequence 1 1
switch(config-acl-ip)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action                    L3 Protocol
          Source IP Address         Source L4 Port(s)
          Destination IP Address    Destination L4 Port(s)
          Additional Parameters
-----
IPv6      MY_IPV6_ACL
1 permit any 2001::1/64                udp
2 Permit all TCP ephemeral ports
  permit 2001:2001::2:1                tcp
  any                                         > 1023
3 permit 2001:2011::1/64                tcp
  any
4 deny any any
  any
  Hit-counts: enabled
Type      Name
Sequence  Comment
          Action                    L3 Protocol
          Source IP Address         Source L4 Port(s)
          Destination IP Address    Destination L4 Port(s)
          Additional Parameters
-----
IPv6      MY_IPV6_ACL
1 permit any 2001::1/64                udp
2 Permit all TCP ephemeral ports
  permit 2001:2001::2:1                tcp
  any                                         > 1023
3 permit 2001:2011::1/64                tcp
  any
4 deny any any
  any
  Hit-counts: enabled

```

Resequencing a MAC ACL to start at 1 with an increment of 1:

```

switch(config)# access-list mac MY_MAC_ACL resequence 1 1
switch(config-acl-mac)# exit

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action                    EtherType
          Source MAC Address
          Destination MAC Address
          Additional Parameters

```

```

-----
MAC      MY_MAC_ACL
1 permit 1122.3344.5566/ffff.ffff.0000      ipv6
  any
2 permit aaaa.bbbb.cccc                      any
  1111.2222.3333
  QoS Priority Code Point: 4
3 Permit all vlan-40 tagged Appletalk traffic
  permit appletalk
  any
  any
  VLAN: 1
4 deny   any
  any
  Hit-counts: enabled

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

access-list reset

`access-list {all|ip <ACL-NAME>|ipv6 <ACL-NAME>|mac <ACL-NAME>} reset`

Description

Changes the user-specified ACL configuration to match the active ACL configuration. Use this command when a discrepancy exists between what the user configured and what is active and accepted by the system.

Parameter	Description
<code>all ip <ACL-NAME> ipv6 <ACL-NAME> mac <ACL-NAME></code>	Specifies one of the following: - a reset of all ACLs. - a reset of a named IPv4 ACL. - a reset of a named IPv6 ACL. - a reset of a named MAC ACL.

Usage

The output of the **show access-list** command displays the active configuration of the product. The active configuration is the ACLs that have been configured and accepted by the system. The output of the **show access-list** command with the **configuration** parameter, displays the ACLs that have been configured. The output of this command may not be the same as what was programmed in hardware or what is active on the product.

If the active ACLs and user-configured ACLs are not the same, a warning message is displayed in the output of the show command. Modify the user-configured ACL until the warning message is no longer displayed or run the **access-list reset** command to change the user-specified configuration to match the active configuration.

Examples

Apply an ACL with TCP acknowledgments (ACKs) on ingress, which is unsupported by hardware:

```
switch(config-acl)# 10 permit tcp 172.16.2.0/16 any ack
```

Displaying the user-specified configuration:

```
switch(config)# do show access-list commands
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
access-list ip TEST_ACL
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
interface 1/1/1
    apply access-list ip TEST_ACL in

switch(config)# do show access-list commands configuration
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
access-list ip TEST_ACL
    10 permit tcp 172.16.2.0/255.255.0.0 any ack
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
interface 1/1/1
    apply access-list ip TEST_ACL in

switch(config)# do show access-list
Type          Name
Sequence      Comment
              Action
              Source IP Address
              Destination IP Address
              Additional Parameters
-----
% Warning: TEST_ACL user configuration does not match active configuration.
%      run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
IPv4          TEST_ACL

switch(config)# do show access-list configuration
Type          Name
Sequence      Comment
```

```

        Action                               L3 Protocol
        Source IP Address                     Source L4 Port(s)
        Destination IP Address                 Destination L4 Port(s)
        Additional Parameters
-----
% Warning: TEST_ACL user configuration does not match active configuration.
%      run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
IPv4      TEST_ACL
          10
            permit                               tcp
            172.16.2.0/255.255.0.0
            any
            ack

! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
access-list ip TEST_ACL
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
interface 1/1/1
    apply access-list ip TEST_ACL in

switch(config)# do show access-list commands configuration
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
access-list ip TEST_ACL
    10 permit tcp 172.16.2.0/255.255.0.0 any ack
! access-list ip TEST_ACL user configuration does not match active configuration.
! run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
interface 1/1/1
    apply access-list ip TEST_ACL in

switch(config)# do show access-list
Type      Name
Sequence Comment
        Action                               L3 Protocol
        Source IP Address                     Source L4 Port(s)
        Destination IP Address                 Destination L4 Port(s)
        Additional Parameters
-----
% Warning: TEST_ACL user configuration does not match active configuration.
%      run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
IPv4      TEST_ACL

switch(config)# do show access-list configuration
Type      Name
Sequence Comment
        Action                               L3 Protocol
        Source IP Address                     Source L4 Port(s)
        Destination IP Address                 Destination L4 Port(s)
        Additional Parameters
-----
% Warning: TEST_ACL user configuration does not match active configuration.
%      run 'access-list TYPE NAME reset' to reset access-list to match active
configuration.
IPv4      TEST_ACL

```

```

10
  permit                                tcp
  172.16.2.0/255.255.0.0
  any
  ack

```

Resetting the user-specified configuration to match the active configuration.

```
switch(config)# access-list ip TEST_ACL reset
```

Displaying the updated user-specified configuration.

```

switch(config)# do show access-list commands
access-list ip TEST_ACL
interface 1/1/1
  apply access-list ip TEST_ACL in

switch(config)# do show access-list commands configuration
access-list ip TEST_ACL
interface 1/1/1
  apply access-list ip TEST_ACL in

switch(config)# do show access-list
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      TEST_ACL

switch(config)# do show access-list configuration
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      TEST_ACL

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

access-list secure-update

```
access-list secure-update
no access list secure-update
```

Description

This command determines if access lists are updated using the secure-update feature. Secure-update is enabled by default.

When secure update is enabled and an ACL is updated or replaced, one or more override entries are installed in the TCAM table(s) containing the ACL that is being modified. As a result, all traffic of the same type as the currently configured ACL will be denied on the interfaces to which the ACL is applied. This ensures that traffic is not temporarily allowed while modifying an ACL. Upon completion of the update, the TCAM override entries are uninstalled and traffic resumes ACL matching.

The **no** version of this command disables this feature. If secure-update is disabled, there will be no override entry installed. This results in the faster modification of an ACL and ensures that there is no interruption to previously permitted traffic, but may temporarily allow previously denied traffic to pass through the switch. Once the ACL has been modified, traffic will be processed by the updated ACL.

Examples

Disabling secure update:

```
switch(config)# no access-list secure-update
```

Reenabling secure update:

```
switch(config)# access-list secure-update
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Related Commands

Command	Description
<code>vsx-sync acl-secure-update</code>	If this setting is enabled and the primary VSX node has configurations with the access list secure-update feature enabled, this configuration can synchronize to the secondary peer. This setting is disabled by default. Refer to the <i>VSX Guide</i> for details.

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

apply access-list control-plane

```
apply access-list {ip|ipv6} <ACL-NAME> control-plane vrf <VRF-NAME>  
no apply access-list {ip|ipv6} <ACL-NAME> control-plane vrf <VRF-NAME>
```

Description

Applies an ACL to the specified VRF.

The **no** form of this command removes application of the ACL from the specified VRF.

Parameter	Description
ip ipv6	Specifies the ACL type: ip for IPv4, or ipv6 for IPv6.
<ACL-NAME>	Specifies the ACL name.
vrf <VRF-NAME>	Specifies the VRF name.

Usage

Only one ACL per type (**ip**, or **ipv6**) may be applied to a Control Plane VRF at a time. Therefore, using the **apply access-list control-plane** command on a VRF with an already-applied ACL of the same type, will replace the applied ACL.

Examples

Applying **My_ip_ACL** to Control Plane traffic on the default VRF:

```
switch(config)# apply access-list ip My_ip_ACL control-plane vrf default
```

Replacing My_ip_ACL with **My_Replacement_ACL** on the default VRF:

```
switch(config)# apply access-list ip My_Replacement_ACL control-plane vrf default
```

Remove (unapply) the **My_Replacement_ACL** from the default VRF. Any other interfaces or VLANs with My_Replacement_ACL applied are unaffected.

```
switch(config)# no apply access-list ip My_Replacement_ACL control-plane vrf default
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

apply access-list (to interface or LAG)

```
no apply access-list {ip | ipv6 | mac} <ACL-NAME> {in | out}
```

Description

Applies an ACL to the interface (Individual front plane port) or Link Aggregation Group (LAG) identified by the current interface or LAG context.

The **no** form of this command removes application of the ACL from the current interface or LAG identified by the current interface or LAG context.

Parameter	Description
ip ipv6 mac	Specifies the ACL type: <code>ip</code> for IPv4, <code>ipv6</code> for IPv6, or <code>mac</code> for MAC ACL.
<ACL-NAME>	Specifies the ACL name.
in	Selects the inbound (ingress) traffic direction.
out	Selects the outbound (egress) traffic direction.

Usage

- Each ACL of a given type can be applied to the same interface or LAG once in each direction. Therefore, using the **apply access-list** command on an interface or LAG with an already-applied ACL of the same type will replace the currently applied ACL.
- An ACL can be applied to an individual front plane port or to a Link Aggregation Group (LAG).
- A port that is a member of a LAG with an applied ACL cannot have a different ACL applied to that member port.

- When the port membership of a LAG with an applied ACL is changed, the LAG ACL is automatically applied or removed from that port depending on the modification type.
- Logging on outbound (egress) traffic is also not supported. An error message will be displayed if an ACL with any logging ACEs is attempted to be applied on egress.

Examples

Applying **My_IP_ACL** to ingress traffic on interface range 1/1/10 to 1/1/12:

```
switch(config)# int 1/1/10-1/1/12
switch((config-if-<1/1/10-1/1/12>)# apply access-list ip My_IP_ACL in
switch((config-if-<1/1/10-1/1/12>)# exit
```

Applying **MY_IP_ACL** to ingress traffic on LAG 100 and egress traffic on interface 1/1/2:

```
switch(config)# interface lag 100
switch(config-lag-if)# apply access-list ip MY_IP_ACL in
switch(config-lag-if)# exit

switch(config)# interface 1/1/2
switch(config-if)# apply access-list ip MY_IP_ACL out
switch(config-if)# exit
switch(config)#
```

Applying **MY_IPV6_ACL** to ingress traffic on interface 1/1/1 and to ingress traffic on LAG 100:

```
switch(config)# interface 1/1/1
switch(config-if)# apply access-list ipv6 MY_IPV6_ACL in
switch(config-if)# exit

switch(config)# interface lag 100
switch(config-lag-if)# apply access-list ipv6 MY_IPV6_ACL in
switch(config-lag-if)# exit
switch(config)#
```

Applying **MY_MAC_ACL** to ingress traffic on interface 1/1/1 and ingress traffic on interface 1/1/2:

```
switch(config)# interface 1/1/1
switch(config-if)# apply access-list mac MY_MAC_ACL in
switch(config-if)# exit

switch(config)# interface 1/1/2
switch(config-if)# apply access-list mac MY_MAC_ACL in
switch(config-if)# exit
switch(config)#
```

Replacing **MY_IP_ACL** with **MY_REPLACEMENT_ACL** on interface 1/1/2:

```
switch(config)# interface 1/1/2
switch(config-if)# apply access-list ip MY_REPLACEMENT_ACL out
switch(config-if)# exit
switch(config)#
```

Unapplying **MY_REPLACEMENT_ACL** from interface 1/1/2 (out):

```
switch(config)# interface 1/1/2
switch(config-if)# no apply access-list ip MY_REPLACEMENT_ACL out
switch(config-if)# exit
switch(config)#
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.11	Egress support extended to 9300 platform.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

apply access-list (to interface VLAN)

```
apply access-list {ip|ipv6} <ACL-NAME> {routed-in|routed-out}
no apply access-list {ip|ipv6} <ACL-NAME> {routed-in|routed-out}
```

Description

Applies an ACL to the interface VLAN (or range of interface VLANs) identified by the current interface VLAN context. Using the apply access-list command on an interface VLAN interface with an already-applied ACL of the same direction and type will replace the currently-applied ACL.

The **no** form of this command removes application of the ACL from the interface VLAN (or range of interface VLANs) identified by the current interface VLAN context.

Parameter	Description
ip ipv6	Specifies the ACL type: ip for IPv4, ipv6 for IPv6.
<ACL-NAME>	Specifies the ACL name.
routed-in	Selects the routed inbound (routed ingress) traffic direction.
routed-out	Selects the routed outbound (routed egress) traffic direction.

Usage

- Each ACL of a given type can be applied to the same interface VLAN once in each direction. Therefore, using the `apply access-list` command on an interface VLAN with an already-applied ACL of the same direction and type, will replace the applied ACL.

Examples

Creating an IPv4 ACL and applying it to routed ingress traffic on interface VLAN `vlan100`:

```
switch(config)# access-list ip test
switch(config-acl-ip)# 10 permit any 1.1.1.2 2.2.2.2 count
switch(config-acl-ip)# 20 permit any 1.1.1.2 2.2.2.1 count
switch(config-acl-ip)# 30 permit any 2.2.2.2 1.1.1.2 count
switch(config-acl-ip)# 40 permit any 2.2.2.2 1.1.1.1 count
switch(config-acl-ip)# 50 permit any any any count
switch(config-acl-ip)# exit
switch(config)#
switch(config)# interface vlan100
switch(config-if-vlan)# apply access-list ip test routed-in
```

Applying `My_ip_ACL` to routed ingress traffic on interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# apply access-list ip My_ip_ACL routed-in
```

Applying `My_ipv6_ACL` to routed ingress traffic on interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# apply access-list ipv6 My_ip_ACL routed-in
```

Applying `My_ip_ACL` to routed ingress traffic on interface VLANs 20 to 25:

```
switch(config)# interface vlan 20-25
switch(config-if-vlan-<20-25># apply access-list ip My_ip_ACL routed-in
```

Replacing `My_ipv6_ACL` with `My_Replacement_ACL` on interface VLAN 10 (following the above examples):

```
switch(config)# interface vlan 10
switch(config-if-vlan)# apply access-list ipv6 My_Replacement_ACL routed-in
```

Removing (unapplying) `My_Replacement_ACL` on interface VLAN 10. Any other interfaces or VLANs with `My_Replacement_ACL` applied are not affected:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no apply access-list ipv6 My_Replacement_ACL routed-in
```

Removing (unapplying) `My_ip_ACL` on interface VLANs 20 to 25. Any other interfaces or VLANs with `My_ip_ACL` applied are not affected:

```
switch(config)# interface vlan 20-25
switch(config-if-vlan-<20-25>)# no apply access-list ip My_ip_ACL routed-in
```

Applying My_ip_ACL to routed egress traffic on interface VLAN 30:

```
switch(config)# interface vlan 30
switch(config-if-vlan)# apply access-list ip My_ip_ACL routed-out
```

Applying My_ip_ACL to routed egress traffic on interface VLANs 40 to 50:

```
switch(config)# interface vlan 40-50
switch(config-if-vlan-<40-50>)# apply access-list ip My_ip_ACL routed-out
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

apply access-list (to subinterface)

```
apply access-list {ip|ipv6|mac} <ACL-NAME> {in|out}
no apply access-list {ip|ipv6|mac} <ACL-NAME> {in|out}
```

Description

Applies an ACL to the current port or LAG subinterface context or subinterface context range.

The **no** form of this command removes application of the ACL from the current port or LAG subinterface context or subinterface context range.



An ACL cannot be applied to the parent interface of one or more subinterfaces. This also means that a subinterface cannot be added to an interface if there is an ACL applied.



ACE VLAN IDs cannot be added to ACLs applied to subinterfaces. This also means that an ACL with an ACE matching on a VLAN ID cannot be applied to a subinterface.

Parameter	Description
ip ipv6 mac	Specifies the ACL type: ip for IPv4, ipv6 for IPv6, or mac for MAC ACL.
<ACL-NAME>	Specifies the ACL name.
in	Selects the traffic direction.

Usage

- In the case of a failed ACL application to a subinterface during switch reboot or hotswap, the subinterface will be shut down. Fixing the failure will cause the subinterface to come back up.
- In the case of a failed ACL application to an added subinterface LAG member(s), the entire LAG subinterface will be shut down. Fixing the failure will cause the LAG subinterface to come back up. For this case to occur, the ACL must already be successfully applied to existing subinterface LAG members. This is done to prevent traffic from circumventing the ACL by passing through new LAG members where the ACL was not successfully applied. This only occurs when the LAG spans more than one line card or stack member.

Examples

Applying My_ip_ACL to ingress traffic on subinterface 1/1/1.10:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# apply access-list ip My_ip_ACL in
```

```
switch(config)# interface 1/1/2.8
switch(config-subif)# apply access-list ip My_ip_ACL_egr out
```

Applying My_ipv6_ACL to ingress traffic on subinterface 1/1/1.10:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# apply access-list ipv6 My_ipv6_ACL in
```

Applying My_ip_ACL to ingress traffic on subinterface range 1/1/1.11 to 1/1/1.15:

```
switch(config)# interface 1/1/1.11-1/1/1.15
switch(config-subif-<1/1/1.11-1/1/1.15>)# apply access-list ip My_ip_ACL in
```

Replacing My_ipv6_ACL with My_Replacement_ACL on subinterface 1/1/1.10 (following the above examples):

```
switch(config)# interface 1/1/1.10
switch(config-subif)# apply access-list ipv6 My_Replacement_ACL in
```

Removing (unapplying) My_Replacement_ACL on subinterface 1/1/1.10. Any other interfaces or VLANs with My_Replacement_ACL applied are not affected.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# no apply access-list ipv6 My_Replacement_ACL in
```

Removing (unapplying) My_ip_ACL on subinterface 1/1/1.11 to 1/1/1.15. Any other interfaces or VLANs with My_ip_ACL applied are not affected.

```
switch(config)# interface 1/1/1.11-1/1/1.15
switch(config-subif-<1/1/1.11-1/1/1.15>)# no apply access-list ip My_ip_ACL in
```

Applying My_ip_ACL to ingress traffic on subinterface lag1.10:

```
switch(config)# interface lag1.10
switch(config-subif)# apply access-list ip My_ip_ACL in
```

Removing (unapplying) My_ip_ACL from subinterface lag1.10:

```
switch(config)# interface lag1.10
switch(config-subif)# no apply access-list ip My_ip_ACL in
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced on the 9300 and 9300S Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-subif	Administrators or local user group members with execution rights for this command.

apply access-list (to VLAN)

```
apply access-list {ip|ipv6|mac} <ACL-NAME> {in|out}
no apply access-list {ip|ipv6|mac} <ACL-NAME> {in|out}
```

Description

Applies an ACL to the VLAN identified by the current VLAN context.

The **no** form of this command removes application of the ACL from the VLAN identified by the current VLAN context.

Parameter	Description
ip ipv6 mac	Specifies the ACL type: ip for IPv4, ipv6 for IPv6, or mac for MAC ACL.
<ACL-NAME>	Specifies the ACL name.
in	Selects the inbound (ingress) traffic direction.
out	Selects the outbound (egress) traffic direction. NOTE: For HPE Aruba Networking 6000 and 6100 Switch series, the outbound (egress) traffic direction is supported only for MAC ACLs.

Usage

Each ACL of a given type can be applied to the same VLAN once in each direction. Therefore, using the **apply access-list** command on a VLAN with an already-applied ACL of the same type, will replace the applied ACL.

Examples

Applying My_ip_ACL to ingress traffic on VLAN range 20 to 25:

```
switch(config)# vlan 20-25
switch(config-vlan-<20-25>)# apply access-list ip My_ip_ACL in
```

Applying My_ip_ACL to egress traffic on VLAN range 40 to 50:

```
switch(config)# vlan 40-50.
switch(config-vlan-<40-50>)# apply access-list ip My_ip_ACL out
```

Applying My_ip_ACL to ingress traffic on VLAN 10:

```
switch(config)# vlan 10
switch(config-vlan-10)# apply access-list ip My_ip_ACL in
```

Applying My_ipv6_ACL to ingress traffic on VLAN 10:

```
switch(config)# vlan 10
switch(config-vlan-10)# apply access-list ipv6 My_ipv6_ACL in
```

Applying My_mac_ACL to ingress traffic on VLAN 10:

```
switch(config)# vlan 10
switch(config-vlan-10)# apply access-list mac My_mac_ACL in
```

Replacing My_ipv6_ACL with My_Replacement_ACL on VLAN 10 (following the preceding examples):

```
switch(config)# vlan 10  
switch(config-vlan-10)# apply access-list ipv6 My_Replacement_ACL in
```

Removing (unapplying, Specifies the ACL type: **ip** for IPv4, **ipv6** for IPv6, or **mac** for MAC ACL.) several ACLs on VLAN 10:

```
switch(config)# vlan 10  
switch(config-vlan-10)# no apply access-list ipv6 My_Replacement_ACL in  
switch(config-vlan-10)# no apply access-list mac My_mac_ACL in
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan	Administrators or local user group members with execution rights for this command.

clear access-list hitcounts

```
clear access-list hitcounts { all | [{ip|ipv6|mac} <ACL-NAME>]  
                             [interface <IF-NAME>| vlan <VLAN-ID>] [in|out|routed-in|routed-out] }
```

Description

Clears the hit counts for ACLs with ACEs that include the `count` keyword.

Parameter	Description
<code>all</code>	Selects all ACLs.
<code>ip ipv6 mac</code>	Specifies the ACL type: <code>ip</code> for IPv4, <code>ipv6</code> for IPv6, or <code>mac</code> for MAC.
<code><ACL-NAME></code>	Specifies the ACL name.
<code>interface <IF-NAME></code>	Specifies the interface name (port or LAG).
<code>vlan <VLAN-ID></code>	Specifies the VLAN.
<code>in</code>	Selects the inbound (ingress) traffic direction.
	Selects the outbound (egress) traffic direction. Available for IPv4

Parameter	Description
	and IPv6 ACLs applied to VLANs and for IPv4 ACLs applied to route-only ports. Not available for ACLs applied to either IPv4 bridged ports or IPv6 ports, or for MAC ACLs applied to ports or VLANs.
routed-in routed-out	Selects the routed traffic direction on which the ACL is applied. NOTE: This is only available for IPv4 and IPv6 ACLs applied to interface VLANs. ▪ routed-in selects the routed inbound (routed ingress) traffic direction. ▪ routed-out selects the routed outbound (routed egress) traffic direction.

Examples

Clearing the hit counts for My_ip_ACL applied to port 1/1/2 (egress):

```
switch# clear access-list hitcounts ip My_ip_ACL interface 1/1/2 out
```

Clearing the hit counts for My_ip_ACL applied to VLAN 10 (ingress):

```
switch# clear access-list hitcounts ip My_ip_ACL vlan 10 in
```

Clearing the hit counts for all ACLs:

```
switch# clear access-list hitcounts all
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear access-list hitcounts control-plane

clear access-list hitcounts [{ip|ipv6} <ACL-NAME>] control-plane vrf <VRF-NAME>

Description

Clears the hit counts for ACLs applied to the Control Plane VRF.

Parameter	Description
ip ipv6	Specifies the ACL type: ip for IPv4, or ipv6 for IPv6.
<ACL-NAME>	Specifies the ACL name.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Clearing the hit counts for an IPv4 ACL applied to the Control Plane default VRF:

```
switch# clear access-list hitcounts ip My_ipv4_ACL control-plane vrf default
```

Clearing the hit counts for an IPv6 ACL applied to the Control Plane default VRF:

```
switch# clear access-list hitcounts ipv6 My_ipv6_ACL control-plane vrf default
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

object-group address resequence

object-group {ip|ipv6} address <OBJECT-GROUP-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>

Description

Reorders the sequence numbers in an address object group.

Parameter	Description
ip ipv6	Specifies the object group IP address type, either ip or ipv6.
<OBJECT-GROUP-NAME>	Specifies the address object group name.
<STARTING-SEQUENCE-NUMBER>	Specifies the starting sequence number.
<INCREMENT>	Specifies the sequence number increment.

Examples

Resequencing address object group my_ipv4_addr_group to use sequence numbers 5, 10, 15 and so on:

```
switch(config)# object-group address my_ipv4_addr_group resequence 5 5
switch(config)#
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

object-group address reset

```
object-group {ip|ipv6} address <OBJECT-GROUP-NAME> reset
```

Description

Resets the user configuration back to the active configuration. This command takes immediate effect, it is not saved in the user configuration. Use this command if misconfiguration of an address object group has occurred.

Parameter	Description
ip ipv6	Specifies the object group IP address type, either ip or ipv6.
<OBJECT-GROUP-NAME>	Specifies the address object group name.

Examples

Resetting IPv4 address object group my_ipv4_group:

```
switch(config)# object-group ip address my_ip_group reset
switch(config)#
```

Resetting IPv6 address object group my_ipv6_group:

```
switch(config)# object-group ipv6 address my_ipv6_group reset
switch(config)#
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

object-group all reset

object-group all reset

Description

Resets the user configuration back to the active configuration for all object types (address and port). This command takes immediate effect, it is not saved in the user configuration. Use this command if misconfiguration of address object groups and port object groups has occurred. Individual address and port object groups can be reset respectively with the **object-group address reset** and **object-group port reset** commands.

Examples

Resetting the user configuration for all object types (address and port):

```
switch(config)# object-group all reset
switch(config)#
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

object-group ip address

Syntax to create an IPv4 address object group and enter its context:

```
object-group ip address <OBJECT-GROUP-NAME>
no object-group ip address <OBJECT-GROUP-NAME>
```

Syntax (within the address object-group context) for creating or removing IPv4 address entries :

```
[ <SEQUENCE-NUMBER>] <IP-ADDRESS>[ / { <PREFIX-LENGTH> | <SUBNET-MASK> } ]
```

```
no <SEQUENCE-NUMBER>
```

Description

Creates an IPv4 address object group comprised of one or more address entries. Address groups are used solely as a shorthand way of specifying groups of addresses in the ACEs that make up ACLs. IPv4 address groups can be used only in the **access-list ip** command. Entering **object-group ip address** with an existing address group name, enables you to modify an existing address group.

The **no** form of this command deletes the entire address group or deletes a particular address group entry identified by sequence number.

Parameter	Description
<OBJECT-GROUP-NAME>	Specifies the address object group name.
<SEQUENCE-NUMBER>	Specifies a sequence number for the address entry. Range: 1 to 4294967295. When omitted, a sequence number 10 larger than the current highest sequence number is auto-assigned. Default auto-assigned sequence numbers are 10, 20, 30, and so on.
<IP-ADDRESS>[/ { <PREFIX-LENGTH> <SUBNET-MASK> }]	Specifies the IPv4 address. ▪ <IP-ADDRESS> - specifies the IPv4 host address. ▪ <PREFIX-LENGTH> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32. ▪ <SUBNET-MASK> - specifies the address bits to mask (dotted decimal notation).

Examples

Creating an IPv4 address group with two entries:

```

switch(config)# object-group ip address my_ipv4_addr_group
switch(config-addrgroup-ip)# 10 192.168.0.1
switch(config-addrgroup-ip)# 20 192.168.0.2
switch(config-addrgroup-ip)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv4         my_ipv4_addr_group
              10 192.168.0.1
              20 192.168.0.2

```

Adding an entry to an existing IPv4 address group:

```

switch(config)# object-group ip address my_ipv4_addr_group
switch(config-addrgroup-ip)# 30 192.168.0.3
switch(config-addrgroup-ip)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv4         my_ipv4_addr_group
              10 192.168.0.1
              20 192.168.0.2
              30 192.168.0.3

```

Removing an entry (20) from an existing IPv4 address group:

```

switch(config)# object-group ip address my_ipv4_addr_group
switch(config-addrgroup-ip)# no 20
switch(config-addrgroup-ip)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv4         my_ipv4_addr_group
              10 192.168.0.1
              30 192.168.0.3

```

Removing an IPv4 address group:

```

switch(config)# no object-group ip address my_ipv4_addr_group
switch(config)# show object-group
No object group found.

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code> The object-group ip address command takes you into the named address group context (with prompt switch (config-addrgroup-ip)#) where you enter the addresses.	Administrators or local user group members with execution rights for this command.

object-group ipv6 address

Syntax to create an IPv6 address object group and enter its context:

```
object-group ipv6 address <OBJECT-GROUP-NAME>
```

```
no object-group ipv6 address <OBJECT-GROUP-NAME>
```

Syntax (within the address object-group context) for creating or removing IPv6 address entries :

```
[ <SEQUENCE-NUMBER>] <IP-ADDRESS>[ / { <PREFIX-LENGTH> | <SUBNET-MASK> } ]
```

```
no <SEQUENCE-NUMBER>
```

Description

Creates an IPv6 address object group comprised of one or more address entries. Address groups are used solely as a shorthand way of specifying groups of addresses in the ACEs that make up ACLs. IPv6 address groups can be used only in the `access-list ipv6` command. Entering `object-group ipv6 address` with an existing address group name, enables you to modify an existing address group.

The **no** form of this command deletes the entire address group or deletes a particular address group entry identified by sequence number.

Parameter	Description
<code><OBJECT-GROUP-NAME></code>	Specifies the address object group name.
<code><SEQUENCE-NUMBER></code>	Specifies a sequence number for the address entry. Range: 1 to 4294967295. When omitted, a sequence number 10 larger than the current highest sequence number is auto-assigned. Default auto-assigned sequence numbers are 10, 20, 30, and so on.
<code><IP-ADDRESS>[/ { <PREFIX-LENGTH> <SUBNET-MASK> }]</code>	Specifies the IPv6 address. ▪ <code><IP-ADDRESS></code> - specifies the IPv6 host address. ◦ <code><PREFIX-LENGTH></code> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 128. ◦ <code><SUBNET-MASK></code> - specifies the address bits to mask (dotted decimal notation).

Examples

Creating an IPv6 address group with two entries:

```
switch(config)# object-group ipv6 address my_ipv6_addr_group
switch(config-addrgroup-ipv6)# 10 1000::1
switch(config-addrgroup-ipv6)# 20 1000::2
switch(config-addrgroup-ipv6)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv6         my_ipv6_addr_group
           10 1000::1
           20 1000::2
```

Adding an entry to an existing IPv6 address group:

```
switch(config)# object-group ipv6 address my_ipv6_addr_group
switch(config-addrgroup-ipv6)#
switch(config-addrgroup-ipv6)# 30 1000::3
switch(config-addrgroup-ipv6)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv6         my_ipv6_addr_group
           10 1000::1
           20 1000::2
           30 1000::3
```

Removing an entry (20) from an existing IPv6 address group:

```
switch(config)# object-group ipv6 address my_ipv6_addr_group
switch(config-addrgroup-ipv6)# no 20
switch(config-addrgroup-ipv6)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv6         my_ipv6_addr_group
           10 1000::1
           30 1000::3
```

Removing an IPv6 address group:

```
switch(config)# no object-group ipv6 address my_ipv6_addr_group
switch(config)# show object-group
No object group found.
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<pre>config</pre> The object-group ipv6 address command takes you into the named address group context (with prompt switch (config-addrgroup-ipv6)#) where you enter the addresses.	Administrators or local user group members with execution rights for this command.

object-group port

Syntax to create a Layer 4 port object group and enter its context:

```
object-group port <OBJECT-GROUP-NAME>
```

```
no object-group port <OBJECT-GROUP-NAME>
```

Syntax (within the port object-group context) for creating or removing Layer 4 port entries:

```
[<SEQUENCE-NUMBER>] { {eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT> }
```

```
no <SEQUENCE-NUMBER>
```

Description

Creates a Layer 4 port object group comprised of one or more port entries. Port groups are used solely as a shorthand way of specifying groups of ports in the ACEs that make up ACLs. Layer 4 port groups can be used only in the **access-list ip** and **access-list ipv6** commands. Entering **object-group port** with an existing port group name, enables you to modify an existing port group.

The **no** form of this command deletes the entire port group or deletes a particular port group entry identified by sequence number.

Parameter	Description
<code><OBJECT-GROUP-NAME></code>	Specifies the port object group name.
<code><SEQUENCE-NUMBER></code>	Specifies a sequence number for the port entry. Range: 1 to 4294967295. When omitted, a sequence number 10 larger than the current highest sequence number is auto-assigned. Default auto-assigned sequence numbers are 10, 20, 30, and so on.
<code>{ {eq gt lt} <PORT> range <MIN-PORT><MAX-PORT> }</code>	Specifies the port or port range. Port numbers are in the range of 0 to 65535. ▪ eq <PORT> - specifies the Layer 4 port. ▪ gt <PORT> - specifies any Layer 4 port greater than the indicated port.

Parameter	Description
	▪ It <PORT> - specifies any Layer 4 port less than the indicated port. ▪ range MIN-PORT> <MAX-PORT> - specifies the Layer 4 port range. NOTE: When ACLs using ACEs defined with port groups are applied, the same number of hardware resources are consumed as when the ports are specified directly in the ACEs and not in a group. Keep this in mind when creating port groups that include many ports. Although hardware resource consumption is the same, with or without port groups used, it may not be immediately obvious that some port groups that you have defined, include many ports. It is recommended that you name port groups in a manner that reminds you that a group includes many ports.

Examples

Creating a port group with two entries to cover port 80 plus ports 0 through 50:

```
switch(config)# object-group port my_port_group
switch(config-portgroup)# 10 eq 80
switch(config-portgroup)# 20 range 0 50
switch(config-portgroup)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
Port          my_port_group
              10 eq 80
              20 range 0 50
```

Adding an entry for ports greater than 65525 (covers ports 65526 through 65535):

```
switch(config)# object-group port my_port_group
switch(config-portgroup)# 30 gt 65525
switch(config-portgroup)# exit
switch(config)# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
Port          my_port_group
              10 eq 80
              20 range 0 50
```

```
30 gt 65525
```

Removing an entry (#20) from the port group:

```
switch(config)# object-group port my_port_group
switch(config-portgroup)# no 20
switch(config-portgroup)# exit
switch(config)# show object-group
Type      Name
Sequence L4 Port(s)/IP Address
-----
Port      my_port_group
          10 eq 80
          30 gt 65525
```

Removing the port group:

```
switch(config)# no object-group port my_port_group
switch(config)# show object-group
No object group found.
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code> The object-group ip port command takes you into the named port group context (with prompt switch(config-portgroup)#) where you specify the ports.	Administrators or local user group members with execution rights for this command.

object-group port resequence

```
object-group port <OBJECT-GROUP-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>
```

Description

Reorders the sequence numbers in a port object group.

Parameter	Description
<code><OBJECT-GROUP-NAME></code>	Specifies the port object group name.
<code><STARTING-SEQUENCE-NUMBER></code>	Specifies the starting sequence number.
<code><INCREMENT></code>	Specifies the sequence number increment.

Examples

Resequencing port object group `my_port_group` to use sequence numbers 110, 120, 130 and so on:

```
switch(config)# object-group port my_port_group resequence 110 10
switch(config)#
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

object-group port reset

`object-group port <OBJECT-GROUP-NAME> reset`

Description

Resets the user configuration back to the active configuration. This command takes immediate effect, it is not saved in the user configuration. Use this command if misconfiguration of a port object group has occurred.

Parameter	Description
<code><OBJECT-GROUP-NAME></code>	Specifies the port object group name.

Examples

Resetting port object group `my_port_group`:

```
switch(config)# object-group port my_port_group reset
switch(config)#
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show access-list

```
show access-list [interface <IF-NAME> | vlan <VLAN-ID> | vni <VNI-ID> | interface vlan
<VLAN-ID> | interface lag <LAG-ID>] [in|out|routed-in|routed-out] [ip|ipv6|mac] [<ACL-
NAME>] [commands] [configuration]
```

```
show access-list [ip|ipv6|mac] [<ACL-NAME>] control-plane [vrf <VRF-NAME>] [commands]
[configuration] [vsx-peer]
```

Description

Shows information about your defined ACLs and where they have been applied. When **show access-list** is entered without parameters, information for all ACLs is shown. The parameters filter the list of ACLs for which information is shown.

Available filtering includes:

- The content of a specific ACL.
- All ACLs of a specific type.
- The ACL applied in a particular direction.
- The ACL applied to a specific interface (port or split port or LAG).
- The ACL applied to a specific VLAN.
- The ACL applied to specific interface VLAN (routed-in or routed-out).
- The control-plane ACL applied to a specific VRF.

Parameter	Description
interface <IF-NAME>	Specifies the interface name (port or LAG).
vlan <VLAN-ID>	Specifies the VLAN.

Parameter	Description
vni <VNI-ID>	Specifies the ID of the VNI.
interface vlan <VLAN-ID>	Specifies a valid 802.1Q VLAN ID. Range: 1 to 4094.
interface lag <LAG-ID>	Specifies a valid LAG ID. Range: 1 to 256.
in	Selects the inbound (ingress) traffic direction.
out	Selects the outbound (egress) traffic direction. Available for IPv4 and IPv6 ACLs applied to VLANs and for IPv4 ACLs applied to route-only ports. Not available for ACLs applied to either IPv4 bridged ports or IPv6 ports, or for MAC ACLs applied to ports or VLANs.
routed-in	Selects the routed inbound (routed ingress) traffic direction. NOTE: This is only available for IPv4 and IPv6 ACLs applied to interface VLANs.
routed-out	Selects the routed outbound (routed egress) traffic direction. NOTE: This is only available for IPv4 and IPv6 ACLs applied to interface VLANs.
ip ipv6 mac	Specifies the ACL type: ▪ ip for IPv4, ▪ ipv6 for IPv6, or ▪ mac for MAC.
<ACL-NAME>	Specifies the ACL name.
commands	Specifies that the ACL definition is to be shown as the commands and parameters used to create it rather than in tabular form.
configuration	Specifies that the user-configured ACLs be shown as entered, even if the ACLs are not active due to ACE-definition command issues or hardware issues. This parameter is useful if there is a mismatch between the entered configuration and the previous successfully programmed (active) ACLs configuration.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Creating an IPv4 ACL, applying it to an interface VLAN (routed in), and then showing ACL information filtered for that interface VAN:

```
switch(config)# access-list ip test
switch(config-acl-ip)# 10 permit any 1.1.1.2 2.2.2.2 count
switch(config-acl-ip)# 20 permit any 1.1.1.2 2.2.2.1 count
switch(config-acl-ip)# 30 permit any 2.2.2.2 1.1.1.2 count
switch(config-acl-ip)# 40 permit any 2.2.2.2 1.1.1.1 count
switch(config-acl-ip)# 50 permit any any any count
```

```

switch(config-acl-ip)# exit
switch(config)#
switch(config)# interface vlan100
switch(config-if-vlan)# apply access-list ip test routed-in
switch(config-if-vlan)# exit
switch(config)# show access-list interface vlan100 ip routed-in

```

Direction

Type	Name	Sequence	Comment	Ac	L3 Protocol	Source IP Address	Destination IP Address	Additional Parameters	Source L4 Port(s)	Destination L4 Port(s)

Routed Inbound

IPv4	test									
		10	permit						any	
			1.1.1.2							
			2.2.2.2							
			Hit-counts: enabled							
		20	permit						any	
			1.1.1.2							
			2.2.2.1							
			Hit-counts: enabled							
		30	permit						any	
			2.2.2.2							
			1.1.1.2							
			Hit-counts: enabled							
		40	permit						any	
			2.2.2.2							
			1.1.1.1							
			Hit-counts: enabled							
		50	permit						any	
			any							
			any							
			Hit-counts: enabled							

Showing an IPv4 ACL:

```

switch# show access-list ip MY_ACL

```

Type	Name	Sequence	Comment	Action	L3 Protocol	Source IP Address	Destination IP Address	Additional Parameters	Source L4 Port(s)	Destination L4 Port(s)

IPv4	MY_ACL									
		10	permit		udp					
			any							
			172.16.1.0/255.255.255.0							
		20	permit		tcp				> 1023	
			172.16.2.0/255.255.0.0							
			any							

```

30 permit                                tcp
   172.26.1.0//255.255.255.0
   any
   syn
   ack
   dscp 10
40 deny                                any
   any
   any
Hit-counts: enabled
-----

```

Showing an IPv4 ACL as commands:

```

switch# show access-list ip MY_ACL commands
access-list ip MY_ACL
  10 permit udp any 172.16.1.0/255.255.255.0
  20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any
  30 permit tcp 172.26.1.0/255.255.255.0 any syn ack dscp 10
  40 deny any any any count

```

Showing IPv4 ACLs applied to VLAN 10, inbound:

```

switch# show access-list vlan 10 ip in
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      My_ip_ACL
  10 permit                                udp
   any
   172.16.1.0/255.255.255.0
  20 permit                                tcp
   172.16.2.0/255.255.0.0
   any
   > 1023
  30 permit                                tcp
   172.26.1.0//255.255.255.0
   any
   syn
   ack
   dscp 10
  40 deny                                any
   any
   any
Hit-counts: enabled
-----

```

Showing IPv6 ACLs applied to LAG 128, inbound:

```

switch# show access-list interface lag128 ipv6 in
Type      Name
Sequence  Comment
          Action
          Source IP Address
          L3 Protocol
          Source L4 Port(s)

```


	Destination IP Address Additional Parameters	Destination L4 Port(s)

IPv6	MY_IPV6_ACL	
10	permit any 2001::1/64	udp
20	permit 2001:2001::2:1/128 any	tcp > 1023
30	permit 2001:2011::1/64	tcp
40	deny any any	any
	Hit-counts: enabled	

Showing an IPv6 ACL as commands:

```
switch# show access-list ipv6 MY_IPV6_ACL commands
access-list ipv6 MY_IPV6_ACL
  10 permit udp any 2001::1/64
  20 permit tcp 2001:2001::2:1/128 gt 1023 any
  40 deny any any any count
```

Showing a MAC ACL:

```
switch# show access-list mac MY_MAC_ACL
Type      Name
Sequence  Comment
          Action
          Source MAC Address
          Destination MAC Address
          Additional Parameters
-----
MAC       MY_MAC_ACL
10 permit 1122.3344.5566/ffff.ffff.0000    ipv6
   any
20 permit aaaa.bbbb.cccc 1111.2222.3333      any
   QoS Priority Code Point: 4
30 deny   any
   any
   Hit-counts: enabled
-----
```

Showing a MAC ACL as commands:

```
switch# show access-list mac MY_MAC_ACL commands
access-list mac MY_MAC_ACL
  10 permit 1122.3344.5566/ffff.ffff.0000 any ipv6
  20 permit aaaa.bbbb.cccc 1111.2222.3333 any pc 4
  30 deny any any any count
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.17	Added new parameters for the 9300 and 9300S Switch Series.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show access-list control-plane

```
show access-list [ip|ipv6] [<ACL-NAME>] control-plane [vrf <VRF-NAME>]
                  [commands] [configuration] [vsx-peer]
```

Description

Shows information about your defined ACLs that have been applied to the Control Plane. When **show access-list control-plane** is entered without parameters, information for all ACLs applied to the Control Plane is shown. The parameters filter the list of ACLs for which information is shown.

Available filtering includes:

- The content of a specific ACL that has been applied to the Control Plane.
- All ACLs of a specific type that have been applied to the Control Plane.
- All ACLs applied to the Control Plane for a specific VRF.

Parameter	Description
ip ipv6	Specifies the ACL type: ip for IPv4, or ipv6 for IPv6.
<ACL-NAME>	Specifies the ACL name.
vrf <VRF-NAME>	Specifies the VRF name.
[commands]	Specifies that the ACL definition is to be shown as the commands and parameters used to create it rather than in tabular form.
[configuration]	Specifies that the user-configured ACLs be shown as entered, even if the ACLs are not active due to ACE-definition command issues or hardware issues. This parameter is useful if there is a mismatch between the entered configuration and the previous

Parameter	Description
	successfully programmed (active) ACLs configuration.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing an IPv4 ACL applied to the Control Plane default VRF:

```
switch# show access-list ip My_ipv4_ACL control-plane vrf default
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv4      My_ipv4_ACL
10 permit                                udp
   any
   172.16.1.0/24
20 permit                                tcp
   172.16.2.0/16
   any
   > 1023
30 permit                                tcp
   172.26.1.0/24
   any
   syn
   ack
   dscp 10
40 deny                                    any
   any
   any
Hit-counts: enabled
-----
```

Showing an IPv6 ACL applied to the Control Plane default VRF:

```
switch# show access-list ipv6 My_ipv6_ACL control-plane vrf default
Type      Name
Sequence  Comment
          Action
          Source IP Address
          Destination IP Address
          Additional Parameters
-----
IPv6      My_ipv6_ACL
10 permit                                udp
   any
   2001::1/64
20 permit                                tcp
   2001:2001::2:1/128
   any
   > 1023
30 permit                                tcp
   2001:2011::1/64
```

```
40 deny                                any
   any
   any
   Hit-counts: enabled
-----
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show access-list hitcounts

For 6300, 6400, 8320, 8325, 8325H, 8325P, 9300 and 9300 Switch series:
show access-list hitcounts { [{ip|ipv6|mac} <ACL-NAME>] [interface <IF-NAME> | vlan <VLAN-ID> | vni <VNI-ID> | interface vlan <VLAN-ID> | interface lag <LAG-ID>] [in|out|routed-in|routed-out]] [vsx-peer] }

Description

Shows the hit count of the number of times an ACL has matched a packet or frame for ACEs with the **count** keyword. For ACEs without the **count** keyword, a dash is shown in place of a hit count.

Parameter	Description
ip ipv6 mac	Specifies the ACL type: ip for IPv4, ipv6 for IPv6, or mac for MAC.
<ACL-NAME>	Specifies the ACL name.
interface <IF-NAME>	Specifies the interface name (port or split port or LAG).
vlan <VLAN-ID>	Specifies the VLAN.
vni <VNI-ID>	Specifies the ID of the VNI.
interface vlan <VLAN-ID>	Specifies a valid 802.1Q VLAN ID. Range: 1 to 4094.

Parameter	Description
<code>interface lag <LAG-ID></code>	Specifies a valid LAG ID. Range: 1 to 256.
<code>in</code>	Selects the inbound (ingress) traffic direction.
<code>out</code>	Selects the outbound (egress) traffic direction. Available for IPv4 and IPv6 ACLs applied to VLANs and for IPv4 ACLs applied to route-only ports. Not available for ACLs applied to either IPv4 bridged ports or IPv6 ports, or for MAC ACLs applied to ports or VLANs.
<code>routed-in</code>	Selects the routed inbound (routed ingress) traffic direction.
<code>routed-out</code>	Selects the routed outbound (routed egress) traffic direction.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

- ACL hit counts are aggregated across all:
 - Physical interfaces to which the ACL is applied to on ingress.
 - Physical interfaces to which the ACL is applied to on egress.
 - VLANs to which the ACL is applied to on ingress.
 - VLANs to which the ACL is applied to on egress.
 - Interface VLANs to which the IPv4 or IPv6 ACL is applied on routed ingress.
 - Interface VLANs to which the IPv4 or IPv6 ACL is applied on routed egress.
- If an ACL with an ACE with the **count** keyword is applied to multiple physical interfaces or VLANs, the hit counts are aggregated. There is one aggregation for physical interfaces and another for VLANs.
- Accumulated hit counts for an applied ACL are cleared upon any modification of the ACL.

Examples

Showing the hit counts for **My_ip_ACL** applied to port 1/1/2:

```
switch# show access-list hitcounts ip My_ip_ACL interface 1/1/2
Statistics for ACL My_ip_ACL (ipv4):
interface 1/1/1-1/1/2,lag1 (out):
    Matched Packets  Configuration
                    - 10 permit udp any 172.16.1.0/255.255.255.0
                    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
                    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
                    0 implicit deny any any any count
```

Showing the hit counts for **My_ip_ACL** applied to VLAN 10:

```
switch# show access-list hitcounts ip My_ip_ACL vlan 10
Statistics for ACL My_ip_ACL (ipv4):
vlan 10,20-100,300 (in):
    Matched Packets  Configuration
```

```

- 10 permit udp any 172.16.1.0/255.255.255.0
0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
- 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
0 implicit deny any any any count

```

Showing the hit counts for **My_ip_ACL** applied to interface VLAN 10:

```

switch# show access-list hitcounts ip My_ip_ACL vlan 10
Statistics for ACL My_ip_ACL (ipv4):
interface vlan 10,20,30 (routed-in):
  Matched Packets  Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count

```

Showing the hit counts for My_ip_ACL applied on any interface and direction:

```

switch# show access-list hitcounts ip My_ip_ACL vlan 10
switch# show access-list hitcounts ip My_ip_ACL
Statistics for ACL My_ip_ACL (ipv4):
interface 1/1/1 (in):
  Matched Packets  Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count

interface 1/1/4.1,1/1/10.10 (in):
  Matched Packets  Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count

interface vlan 10,20,30 (routed-in):
  Matched Packets  Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count

interface vlan 80-85 (routed-out):
  Matched Packets  Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count

vlan 10,20-100,300 (in):
  Matched Packets  Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count

```

```
vrf blue,default,red (control-plane):
  Matched Packets Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count
```

Showing hit counts for **My_ip_ACL** applied to L3 VNIs.

```
switch# show access-list hitcounts ip My_ip_ACL vni 10
Statistics for ACL My_ip_ACL (ipv4):
vni 10 (routed-in):
  Matched Packets Configuration
    - 10 permit udp any 172.16.1.0/255.255.255.0
    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
    0 implicit deny any any any count
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.17	Added support for L3 VNI ACLs on the 9300 and 9300S Switch Series.
10.07 or earlier	Updated command output to use interface and VLAN ranges to reflect aggregation.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show access-list hitcounts control-plane

```
show access-list hitcounts [{ip|ipv6} <ACL-NAME>] control-plane vrf <VRF-NAME> [vsx-peer]
```

Description

Shows the hit count of the number of times an ACL (applied to the Control Plane) has matched a packet for ACEs with the `count` keyword. For ACEs without the `count` keyword, a dash is shown in place of a hit count.

Parameter	Description
ip ipv6	Specifies the ACL type: ip for IPv4, or ipv6 for IPv6.
<ACL-NAME>	Specifies the ACL name.
vrf <VRF-NAME>	Specifies the VRF name.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

- ACL hit counts are aggregated across all VRFs to which the ACL is applied to on ingress.
- Accumulated hit counts for an applied ACL are cleared upon any modification of the ACL.

Examples

Showing the hit counts for an IPv4 ACL applied to the Control Plane default VRF:

```
switch# show access-list hitcounts ip My_ipv4_ACL control-plane vrf default
Statistics for ACL My_ip_ACL (ipv4):
vrf default (control-plane):
    Matched Packets  Configuration
                    - 10 permit udp any 172.16.1.0/255.255.255.0
                    0 20 permit tcp 172.16.2.0/255.255.0.0 gt 1023 any count
                    - 30 permit tcp 172.26.1.0/255.255.255.0 any dscp AF11 ack syn
                    0 implicit deny any any any count
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show access-list secure-update

show access-list secure-update

Description

Use this command to determine if access lists are updated using the secure-update feature. Secure update is enabled by default.

Examples

Displaying the status of the access list secure-update feature when that feature is enabled:

```
switch(config)# show access-list secure-update
Access-list secure-update is enabled
```

Displaying the status of the access list secure-update feature when that feature is disabled:

```
switch(config)# show access-list secure-update
Access-list secure-update is disabled
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Related Commands

Command	Description
<code>access-list secure-update</code>	This command determines if access lists are updated using the secure-update feature. Secure-update is enabled by default.

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

show capacities

```
show capacities <FEATURE> [vsx-peer]
```

Description

Shows system capacities and their values for all features or a specific feature.

Parameter	Description
<FEATURE>	Specifies a feature. For example, aaa or vrrp .
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Capacities are expressed in user-understandable terms. Thus they may not map to a specific hardware or software resource or component. They are not intended to define a feature exhaustively.

Examples

Showing all available capacities for BGP:

```
switch# show capacities bgp

System Capacities: Filter BGP
Capacities Name                                     Value
-----
-
Maximum number of AS numbers in as-path attribute
32
...
```

Showing all available capacities for mirroring:

```
switch# show capacities mirroring

System Capacities: Filter Mirroring
Capacities Name                                     Value
-----
-
Maximum number of Mirror Sessions configurable in a system
4
Maximum number of enabled Mirror Sessions in a system
4
```

Showing all available capacities for MSTP:

```
switch# show capacities mstp

System Capacities: Filter MSTP
Capacities Name                                     Value
-----
-
Maximum number of mstp instances configurable in a system
64
```

Showing all available capacities for VLAN count:

```
switch# show capacities vlan-count
```

```
System Capacities: Filter VLAN Count  
Capacities Name
```

```
Value
```

```
-----  
-
```

```
Maximum number of VLANs supported in the system  
4094 /switch# show capacities vlan-count
```

```
System Capacities: Filter VLAN Count  
Capacities Name
```

```
Value
```

```
-----  
-
```

```
Maximum number of VLANs supported in the system  
4094
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show capacities-status

```
show capacities-status <FEATURE> [vsx-peer]
```

Description

Shows system capacities status and their values for all features or a specific feature.

Parameter	Description
<FEATURE>	Specifies the feature, for example aaa or vrp for which to display capacities, values, and status. Required.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

The number of IP neighbors (IPv4+IPv6) entries section in the output of the **show capacities-status l3-resources** command lists the maximum number of neighbors supported by the platform (with both IPv4 and IPv6 neighbors combined). On HPE Aruba Networking 8320, 8325, 8400, 9300/9300S, 10000

Switch series, IPv6 neighbors will count a value of two for each neighbor, as they take up twice the space in hardware as compared to IPv4 neighbors. In previous releases, the output the **show capacities-status l3-resources** command counted IPv4 and IPv6 neighbors as consuming the same number of resources/space in hardware.



For Spine and L3-core profiles on HPE Aruba Networking 8320, 8325 and 10000 Switch series, the IPv6 Route entry size is still one for each neighbor. For Leaf and L3-aggr profiles, the entry size is also one for IPv6 routes with a prefix greater than 64.

Examples

Showing the system capacities status for all features:

```
switch# show capacities-status

System Capacities Status
Capacities Status Name                                     Value
Maximum
-----
-----
Number of active gateway mac addresses in a system         0
    16
Number of aspath-lists configured                           0
    64
Number of community-lists configured                        0
    64
...

```

Showing the system capacities status for BGP:

```
switch# show capacities-status bgp

System Capacities Status: Filter BGP
Capacities Status Name                                     Value  Maximum
-----
--
Number of aspath-lists configured                           0       64
Number of community-lists configured                         0       64
Number of neighbors configured across all VRFs               0       50
Number of peer groups configured across all VRFs             0       25
Number of prefix-lists configured                           0       64
Number of route-maps configured                             0       64
Number of routes in BGP RIB                                  0      256000
Number of route reflector clients configured across all VRFs 0        16

```

Showing the system capacities status for L3:

```
switch# show capacities-status l3

System Capacities Status: Filter L3 resources
Capacities Status Name                                     Value
Maximum
-----
--
Number of IP neighbor (IPv4+IPv6) entries                    4

```

```

49152
Number of IP Directed Broadcast neighbor entries          0
4096
Number of IPv6 Long Prefix Routes currently configured    3
5000
Number of IPv6 neighbor(ND) entries                      4
49152
Number of L3 Groups for IP Tunnels and ECMP Groups currently configured 1
2047
Number of L3 Destinations for Routes, Nexthops in ECMP groups and
Tunnels currently configured                             4
2045
Number of routes (IPv4+IPv6) currently configured        5
65536
Number of IPv4 routes currently configured               0
65536
Number of IPv6 routes currently configured with prefix 0-64 4
13312
Number of IPv6 routes currently configured with prefix 65-127 2
510

```

```
switch# show capacities-status l3
```

System Capacities Status: Filter L3 resources

Capacities Status Name	Value

Maximum

--	
Number of IP neighbor (IPv4+IPv6) entries	4
49152	
Number of IP Directed Broadcast neighbor entries	0
4096	
Number of IPv6 Long Prefix Routes currently configured	3
5000	
Number of IPv6 neighbor(ND) entries	4
49152	
Number of L3 Groups for IP Tunnels and ECMP Groups currently configured	1
2047	
Number of L3 Destinations for Routes, Nexthops in ECMP groups and Tunnels currently configured	4
2045	
Number of routes (IPv4+IPv6) currently configured	5
65536	
Number of IPv4 routes currently configured	0
65536	
Number of IPv6 routes currently configured with prefix 0-64	4
13312	
Number of IPv6 routes currently configured with prefix 65-127	2
510	



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.13	Updated to show newly supported configuration of IPv6 routes on the ASIC.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show object-group

```
show object-group [{ip|ipv6} address | port] [<OBJECT-GROUP-NAME>] [commands]
[configuration]
```

Description

Shows information about your defined object groups. When **show object-group** is entered without parameters, information for all object groups is shown. The parameters filter the list of object groups for which information is shown.

Parameter	Description
[{ip ipv6} address port]	Specifies the object group type, either address for an IP address, or port .
<OBJECT-GROUP-NAME>	Specifies the object group name.
[commands]	Specifies that the object group definition is to be shown as the commands and parameters used to create it rather than in tabular form.
[configuration]	Specifies that the user-configured object groups be shown as configured. The output of the command with this parameter may not be the same as what is active on the switch due to a misconfigured object group. See <i>Examples</i> in this topic.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing configured object groups:

```
switch# show object-group
Type      Name
Sequence L4 Port(s)/IP Address
-----
IPv4      my_address_group
10 192.168.0.1
```

```

        20 192.168.0.3
Port      my_port_group
        10 eq 80
        20 gt 65525
switch#
switch# show object-group commands
object-group ip address my_address_group
    10 192.168.0.1
    20 192.168.0.3
object-group port my_port_group
    10 eq 80
    20 gt 65525

```

Showing a misconfigured object group:

```

switch# show object-group
Type      Name
Sequence L4 Port(s)/IP Address
-----
! object-group ip address My_ip_object_group user configuration does not match
! the active hardware configuration. Run 'object-group ip address NAME reset'
! to reset the object group to match the active hardware configuration.
IPv4      my_address_group
switch#
switch#
Type      Name
Sequence L4 Port(s)/IP Address
-----
! object-group ip address My_ip_object_group user configuration does not match
! the active hardware configuration. Run 'object-group ip address NAME reset'
! to reset the object group to match the active hardware configuration.
IPv4      my_address_group
switch#
switch# show object-group configuration
Type      Name
Sequence L4 Port(s)/IP Address
-----
! object-group ip address My_ip_object_group user configuration does not match
! the active hardware configuration. Run 'object-group ip address NAME reset'
! to reset the object group to match the active hardware configuration.
IPv4      my_address_group
          10 192.168.0.1
          20 192.168.0.3
switch#
switch# show object-group commands
! object-group ip address My_ip_object_group user configuration does not match
! the active hardware configuration. Run 'object-group ip address NAME reset'
! to reset the object group to match the active hardware configuration.
switch#
switch# show object-group commands configuration
! object-group ip address My_ip_object_group user configuration does not match
! the active hardware configuration. Run 'object-group ip address NAME reset'
! to reset the object group to match the active hardware configuration.
object-group ip address my_address_group
    10 192.168.0.1
    20 192.168.0.3

```

Resetting a misconfigured object group:

```

switch(config)# object-group all reset
switch(config)# exit
switch# show object-group
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv4         my_address_group
switch#
switch# show object-group configuration
Type          Name
Sequence L4 Port(s)/IP Address
-----
IPv4         my_address_group

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show resources

```
show resources [vsx-peer]
```

Description

Shows hardware resource consumption on the switch. Resource data is updated every 10 seconds. Hardware resource consumption information is shown for:

- TCAM entries
- Policers
- L4 Port Ranges

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing hardware resource consumption on a 9300 switch:

```
switch# show resources

Resource Usage:

Mod   Description
      Resource                               Width   Used Reserved   Free
-----
1/1   Global
      Total
      Destination Field Processor Entries      0         0    1024
1/1-0 Ports 9-12,21-24
      Ingress Control Plane Policing
      Ingress TCAM Entries                     3       375    6144
      Total
      Ingress TCAM Entries                     375    6144   18432
      VLAN Field Processor Entries             0         0    1024
1/1-1 Ports 1-8
      Ingress Control Plane Policing
      Ingress TCAM Entries                     3       375    6144
      Total
      Ingress TCAM Entries                     375    6144   18432
      VLAN Field Processor Entries             0         0    1024
1/1-2 Ports 13-20
      Ingress Control Plane Policing
```

	Ingress TCAM Entries	3	375	6144	
Total					
	Ingress TCAM Entries		375	6144	18432
	VLAN Field Processor Entries		0	0	1024
1/1-3 Ports 25-32					
	Ingress Control Plane Policing				
	Ingress TCAM Entries	3	375	6144	
Total					
	Ingress TCAM Entries		375	6144	18432
	VLAN Field Processor Entries		0	0	1024



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

arp ip

```
arp ip <IP_ADDR> mac <MAC_ADDR>
no arp ip <IP_ADDR> mac <MAC_ADDR>
```

Description

Specifies a permanent static neighbor entry in the ARP table (for IPv4 neighbors).
The no form of this command deletes a permanent static neighbor entry from the ARP table.

Parameter	Description
ip <IP-ADDR>	Specifies the IP address of the neighbor or the virtual IP address of the cluster in IP format (x.x.x.x), where x is a decimal number from 0 to 255. . Range: 4096 to 131072. Default: 131072.
mac <MAC-ADDR>	Specifies the MAC address of the neighbor or the multicast MAC address in IANA format (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F. Range: 4096 to 131072. Default: 131072.

Example

Configuring a static ARP entry on a interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# arp ip 2.2.2.2 mac 01:00:5e:00:00:01
```

Removing a static ARP entry on interface VLAN10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no arp ip 2.2.2.2 mac 01:00:5e:00:00:01
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

arp process-grat-arp

```
arp process-grat-arp  
no arp process-grat-arp
```

Description

Enables the processing of gratuitous ARP packets on the individual port or group of L3 ports together. By default, the gratuitous ARP processing is enabled. When gratuitous ARP (GARP) processing is enabled, a switch that is advertising any changes in its MAC through the GARP will reflect in the neighbor table of the switch. However, the switch will not be able to learn the neighbor through the GARP. This configuration is applicable only on L3 interfaces such as ROPs, subinterfaces, and SVIs. The **no** form of this command disables the processing of gratuitous ARP packets.

Example

Enabling the processing of gratuitous ARP packets on the interface **1/1/1**:

```
switch(config)# interface 1/1/1  
switch(config-if)# no shutdown  
switch(config-if)# arp process-grat-arp
```

Enabling the processing of gratuitous ARP packets on interfaces **1/1/1** to **1/1/5**:

```
switch(config)# interface 1/1/1-1/1/5  
switch(config-if<1/1/1-1/1/5>)# no shutdown  
switch(config-if<1/1/1-1/1/5>)# arp process-grat-arp
```

Enabling the processing of gratuitous ARP packets on sub-interface **1/1/1.10**:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10  
switch(config-subif)# no shutdown  
switch(config-subif)# arp process-grat-arp
```

Disabling the processing of gratuitous ARP packets on VLANs **2** to **100**:

```
switch(config)# interface vlan 2-100  
switch(config-if-vlan<2-100>)# no shutdown  
switch(config-if-vlan<2-100>)# no arp process-grat-arp
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-if-vlan config-subif	Administrators or local user group members with execution rights for this command.

clear arp

```
clear arp
port <PORT-ID> [ip <A.B.C.D>|all] [[ipv6 <X:X::X:X>|all]vla
vrf [all-vrfs|{<VRF-NAME> [ip <A.B.C.D>] [[ipv6 <X:X::X:X>]]]
```

Description

Clears IPv4 and IPv6 neighbor entries from the ARP table. If you do not specify any VRF or port parameters, ARP table entries are cleared for the **default** VRF.

Parameter	Description
port <PORT-ID>	Specifies a port on the switch. For example: 1/1/1 .
ip <A.B.C.D> all]	(Optional) Include an IP address to clear neighbor entries for that specific address, or use the all parameter to clear entries for all IP addresses.
ipv6 <X:X::X:X> all	(Optional) Include an IPv6 address to clear neighbor entries for that specific address, or use the all parameter to clear entries for all IPv6 addresses.
vrf	Clears IPv4 and IPv6 neighbor entries for the specified VRF or for all VRFs. If no VRF is specified the default VRF is cleared.
all-vrfs	Clear neighbor entries for all VRFs
<VRF-NAME>	Clear neighbor entries for the specified VRF.
ip <A.B.C.D>	(Optional) Include an IP address to clear just the neighbor entries for the specified IP address.
ipv6 <X:X::X:	(Optional) Include an IPv6 address to clear the neighbor entries for the specified IPv6 address.

Examples

Clearing all IPv4 and IPv6 neighbor ARP entries for the default VRF:

```
switch# clear arp
```

Clearing all ARP neighbor entries for a port:

```
switch# clear arp 1/1/35
```

Clearing all IPv4 and IPv6 neighbor ARP entries for all VRFs:

```
switch# clear arp vrf all-vrfs
```

Clearing all IPv4 and IPv6 neighbor ARP entries for a specific VRF instance:

```
switch# clear arp vrf RED
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

ip local-proxy-arp

```
ip local-proxy-arp  
no ip local-proxy-arp
```

Description

Enables local proxy ARP on the specified interface. Local proxy ARP is supported on Layer 3 physical interfaces and on VLAN interfaces. To enable local proxy ARP on an interface, routing must be enabled on that interface.

The **no ip local-proxy-arp** command disables local proxy ARP on the specified interface.

Examples

Enabling local proxy ARP on interface **1/1/1**:

```
switch# interface 1/1/1  
switch(config-if)# ip local proxy-arp
```

Enabling local proxy ARP on interface VLAN **3**:

```
switch# interface vlan 3
switch(config-if-vlan)# ip local-proxy-arp
```

Disabling local proxy ARP on on interface **1/1/1**.

```
switch# interface 1/1/1
switch(config-if)# no ip local-proxy-arp
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.16	Support added for the 6200 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip proxy-arp

```
ip proxy-arp
no ip proxy-arp
```

Description

Enables proxy ARP for the specified Layer 3 interface. Proxy ARP is supported on Layer 3 physical interfaces, LAG interfaces, and VLAN interfaces. It is disabled by default. To enable proxy ARP on an interface, routing must be enabled on that interface.

The **no** form of this command disables proxy ARP for the specified interface.

Examples

Enabling proxy ARP on interface **1/1/1**:

```
switch# interface 1/1/1
switch(config-if)# ip proxy-arp
```

Enabling proxy ARP on VLAN **3**:

```
switch# interface vlan 3
switch(config-if-vlan)# ip proxy-arp
```

Enabling proxy ARP on a LAG **11**:

```
switch(config)# int lag 11
switch(config-lag-if)# ip proxy-arp
```

Disabling proxy ARP on interface 1/1/1:

```
switch# interface 1/1/1
switch(config-if)# no ip proxy-arp
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-if-vlan config-lag-vlan	Administrators or local user group members with execution rights for this command.

ipv6 local-proxy-nd

```
ipv6 local-proxy-nd
no ipv6 local-proxy-nd
```

Description

Enables local proxy ND for the specified interface.

The **no ipv6 local-proxy-nd** command disables local proxy ND for the specified interface.

Usage

Before enabling local proxy ND, disable Internet Control Message Protocol (ICMP) redirect messages. Disabling the ICMP redirect ensures that hosts don't communicate through other gateways which could possibly have better routes and thereby skip the proxy.

Example

Enable local proxy ND on a L3 physical interface.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 local-proxy-nd
```

Enable local proxy ND on a VLAN interface.


```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 local-proxy-nd
```

Disable local proxy ND for the specified interface.

```
switch(config-if)# no ipv6 local-proxy-nd
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 neighbor mac

```
ipv6 neighbor <IPV6-ADDR> mac <MAC-ADDR>
no ipv6 neighbor <IPV6-ADDR> mac <MAC-ADDR>
```

Description

Specifies a permanent static neighbor entry in the ARP table (for IPv6 neighbors).

The **no** form of this command deletes a permanent static neighbor entry from the ARP table.

Parameter	Description
<IPV6-ADDR>>	Specifies an IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Range: 4096 to 131072. Default: 131072.
mac <MAC-ADDR>>	Specifies the MAC address of the neighbor (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F. Range: 4096 to 131072. Default: 131072.

Example

Creates a static ARP entry on interface **1/1/1**.

```
switch(config)# interface 1/1/1
switch(config-if)# arp ipv6 neighbor 2001:0db8:85a3::8a2e:0370:7334 mac
00:50:56:96:df:c8
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

show arp

```
show arp [vsx-peer]
```

Description

Shows the entries in the ARP (Address Resolution Protocol) table.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

This command displays information about ARP entries, including the IP address, MAC address, port, and state.

When no parameters are specified, the `show arp` command shows all ARP entries for the default VRF (Virtual Router Forwarding) instance.

Examples

```
switch# show arp
```

IPv4 Address	MAC	Port	Physical Port	
192.168.1.2	00:50:56:96:7b:e0	vlan10	1/1/29	stale
192.168.1.3	00:50:56:96:7b:ac	vlan10	1/1/1	reachable

```
Total Number Of ARP Entries Listed- 2.
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show arp state

```
show arp state {all | failed | incomplete | permanent | reachable | stale} [vsx-peer]
```

Description

Shows ARP (Address Resolution Protocol) cache entries that are in the specified state.

Parameter	Description
all	Shows the ARP cache entries for all VRF (Virtual Router Forwarding) instances.
failed	Shows the ARP cache entries that are in <code>failed</code> state. The neighbor might have been deleted.
incomplete	Shows the ARP cache entries that are in <code>incomplete</code> state. An incomplete state means that address resolution is in progress and the link-layer address of the neighbor has not yet been determined. A solicitation request was sent, and the switch is waiting for a solicitation reply or a timeout.
permanent	Shows the ARP cache entries that are in <code>permanent</code> state. ARP entries that are in a permanent state can be removed by administrative action only.
reachable	Shows the ARP cache entries that are in <code>reachable</code> state, meaning that the neighbor is known to have been reachable recently.
stale	Shows ARP cache entries that are in <code>stale</code> state. ARP cache entries are in the <code>stale</code> state if the elapsed time is in excess of the ARP timeout in seconds since the last positive confirmation that the forwarding path was functioning properly.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show arp state failed
```

IPv4 Address	MAC	Port	Physical Port	State
192.168.1.4		vlan10		failed



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show arp summary

```
show arp summary [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows a summary of the IPv4 and IPv6 neighbor entries on the switch for all VRFs or a specific VRF.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing summary ARP information for all VRFs:

```
switch# show arp summary all-vrfs
```

ARP Entry's State	: IPv4	IPv6

Number of Reachable ARP entries	: 2	0
Number of Stale ARP entries	: 0	0
Number of Failed ARP entries	: 2	2
Number of Incomplete ARP entries	: 0	0
Number of Permanent ARP entries	: 0	0

Total ARP Entries: 6	: 4	2

Showing a summary of all IPv4 and IPv6 neighbor entries on the primary and secondary (peer) switches:

```
vsx-primary# show arp summary
```

ARP Entry's State	IPv4	IPv6

Number of Reachable ARP entries	25858	32231
Number of Stale ARP entries	0	1
Number of Failed ARP entries	0	257
Number of Incomplete ARP entries	0	0
Number of Permanent ARP entries	0	0

Total ARP Entries- 58347	25858	32489


```
vsx-primary# show arp summary vsx-peer
```

ARP Entry's State	IPv4	IPv6

Number of Reachable ARP entries	25858	32168
Number of Stale ARP entries	0	3
Number of Failed ARP entries	0	317
Number of Incomplete ARP entries	0	0
Number of Permanent ARP entries	0	0

Total ARP Entries- 58346	25858	32488



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show arp timeout

```
show arp timeout [<INTERFACE>] [vsx-peer]
```

Description

Shows the age-out period for each ARP (Address Resolution Protocol) entry for a port, LAG, or VLAN interface.

Parameter	Description
<INTERFACE>	Specifies a physical port, VLAN, or LAG on the switch. For physical ports, use the format <code>member/slot/port</code> (for example, 1/3/1).
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing ARP timeout information for a port:

```
switch# show arp timeout 1/1/1
ARP Timeout:

-----
Port          VRF          Timeout
1/1/1         default      600
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show arp vrf

show arp {all-vrfs | vrf <VRF-NAME>} [vsx-peer]

Description

Shows the ARP table for all VRF instances, or for the named VRF.

Parameter	Description
all-vrfs	Specifies all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing ARP entries for VRF **vrf1**.

```
switch# show arp vrf vrf1
```

IPv4 Address VRF	MAC	Port	Physical Port	State
100.1.250.50	00:50:56:8d:44:13	vlan1001	1/1/2	reachable
100.2.250.60	00:50:56:8d:45:63	vlan1002	vxlan1 (1920:1680:1:1::2)	permanent

Total Number Of ARP Entries Listed: 2.

This example from a different network shows ARP entries for all VRFs.

```
switch# show arp all-vrfs
```

ARP IPv4 Entries:

IPv4 Address	MAC	Port	Physical Port	State	VRF
192.168.120.10	00:50:56:bd:10:be	1/1/32	1/1/32	reachable	red
10.20.30.40	00:50:56:bd:6a:c5	1/1/29	1/1/29	reachable	test

Total Number Of ARP Entries Listed: 2.



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 neighbors

```
show ipv6 neighbors {all-vrfs | vrf <VRF-NAME>} [vsx-peer]
```

Description

Shows entries in the ARP table for all IPv6 neighbors for all VRFs or for a specific VRF.

When no parameters are specified, this command shows all ARP entries for the default VRF, and state information for `reachable` and `stale` entries only.

Parameter	Description
<code>all-vrfs</code>	Specifies all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show ipv6 neighbors
IPv6 Entries:
```

```
-----
IPv6 Address          MAC                Port      Physical Port  State
fe80::a21d:48ff:fe8f:2700  a0:1d:48:8f:27:00  vlan2300  1/1/31         reachable
fe80::f603:43ff:fe80:a600  f4:03:43:80:a6:00  vlan2300  1/1/30         reachable
-----
```

```
Total Number Of IPv6 Neighbors Entries Listed: 2.
-----
```




For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ipv6 neighbors state

```
show ipv6 neighbors state {all | failed | incomplete | permanent | reachable | stale}
[vsx-peer]
```

Description

Shows all IPv6 neighbor ARP (Address Resolution Protocol) cache entries, or those cache entries that are in the specified state.

Parameter	Description
all	Shows all ARP cache entries.
failed	Shows ARP cache entries that are in <code>failed</code> state. The neighbor might have been deleted. Set the neighbor to be unreachable.
incomplete	Shows ARP cache entries that are in <code>incomplete</code> state. An incomplete state means that address resolution is in progress and the link-layer address of the neighbor has not yet been determined. This means that a solicitation request was sent, and you are waiting for a solicitation reply or a timeout.
permanent	Shows ARP cache entries that are in <code>permanent</code> state.
reachable	Shows ARP cache entries that are in <code>reachable</code> state, meaning that the neighbor is known to have been reachable recently.
stale	Shows ARP cache entries that are in <code>stale</code> state. ARP cache entries are in the <code>stale</code> state if the elapsed time is in excess of the ARP timeout in seconds since the last positive confirmation that the forwarding path was functioning properly.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show ipv6 neighbors state all
```

IPv6 Address	MAC	Port	Physical Port	State
100::2	48:0f:cf:af:f1:cc	lag1	lag1	reachable
300::3	48:0f:cf:af:33:be	vlan3	1/4/20	reachable
fe80::4a0f:cfff:feaf:f1cc	48:0f:cf:af:f1:cc	lag1	lag1	reachable
200::3	48:0f:cf:af:33:be	1/4/11	1/4/11	reachable
fe80::4a0f:cfff:feaf:33be	48:0f:cf:af:33:be	vlan3	1/4/20	reachable

Total Number Of IPv6 Neighbors Entries Listed- 5.



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

hpe-anw-central

```
hpe-anw-central
no hpe-anw-central
```

Description

Creates or enters the HPE Aruba Networking Central configuration context (**config-hpe-anw-central**). When a switch is able to connect to HPE Aruba Networking Central but is not registered in the HPE Aruba Networking Central inventory or does not have a proper license, the switch will get disconnected. If the HPE Aruba Networking Central feature is enabled using this command, the switch will then reconnect back to HPE Aruba Networking Central and will get disconnected again. This connect/disconnect process will continue until the switch is properly registered in HPE Aruba Networking Central. To avoid this unnecessary reconnection cycle, best practices is to disable HPE Aruba Networking Central until the switch is registered in HPE Aruba Networking Central, or a license is obtained for that device.

Example

Creating the HPE Aruba Networking Central configuration context:

```
switch(config)# hpe-anw-central
switch(config-hpe-anw-central)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.15	Command syntax changed from aruba-central to hpe-anw-central .
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

hpe-anw-central support-mode

hpe-anw-central support-mode
no hpe-anw-central support-mode

Description

Allows the device to be writable for all operations in HPE Aruba Networking Central lockout mode for troubleshooting. The no form of this command disables this activity.



Support-mode is disabled by default when the switch is managed by HPE Aruba Networking Central. This command is only effective in the CLI session where it is executed.

Examples

Configuring the device to be writable for all operations in HPE Aruba Networking Central lockout mode:

```
switch# hpe-anw-central support-mode
```

Removing the configuration that allows the device to be writable for all operations in HPE Aruba Networking Central lockout mode:

```
switch# no hpe-anw-central support-mode  
switch#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.15	Command syntax changed from aruba-central to hpe-anw-central .
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

configuration-lockout central managed

configuration-lockout central managed
no configuration-lockout central managed

Description

Configures the device to only be writable from HPE Aruba Networking Central. HPE Aruba Networking Central will be the only agent that can add, modify, or delete configurations on the device. The no form of this command disables this feature.



The no form of this command is only available when the device is disconnected from HPE Aruba Networking Central.

Usage

The AOS-CX switch connects to HPE Aruba Networking Central in either of two modes: monitor or managed. When the device is connected in monitor mode, HPE Aruba Networking Central monitors the configurations on the switch. When the device is connected in managed mode, the **configuration-lockout central managed** command does not allow configuration changes from other interfaces such as CLI or Web UI.

Examples

Configuring the device to only be writable from HPE Aruba Networking Central :

```
switch(config)# configuration-lockout central managed
switch# show configuration-lockout
configuration lockout
-----
central: managed
switch# sh hpe-anw-central
Central admin state           :enable
Central location              :20.0.0.2:8083
VRF for connection            :default
Central connection status     :connected

Central source                 :cli
Central source connection status :connected
Central source last connected on :Tue Feb 9 17:53:13 UTC 2021

Activate Server URL           :devices-v2.arubanetworks.com
CLI location                   :20.0.2:8083
CLI VRF                        :default
switch(config)# end
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

diag-dump rest basic

diag-dump rest basic

Description

Display REST paths and diagnostics information for the REST feature. The output of this command includes diagnostics information for HPE Aruba Networking Central.

Example

The following example displays just the **Central Counters** portion of the output for this command.

```
switch# diag-dump rest basic
=====
[Start] Feature rest Time : Sun Sep 17 17:06:50 2023
=====
...
...
...
Central Counters:
-----
Logins:                                1
Connections:                           1
Disconnections:                         0
-----
Pings:                                 50
Pongs:                                 50
-----
API Requests:                           20
Response API Requests:                  20
-----
v1 Notification Requests Received:      5
v1 Notifications Sent:                  15
Initial Snapshots:                      5
Notifications:                          10
Errors:                                 0
-----
v2 Notification Requests Received:      10
v2 Notifications Sent:                  24
Initial Snapshots:                      10
Unsubscribes:                           0
Notifications:                          14
Errors:                                 0
-----
Views Notification Requests:             0
Views Notification Responses:            0
Views Unary Requests:                   0
Views Unary Responses:                   0
-----
Packet Capture Responses:               0
-----
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
all platforms	config	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables connection to HPE Aruba Networking Central server.

When the connection is disabled, the switch does not attempt to connect to the HPE Aruba Networking Central server or fetch central location from any of the three sources (CLI/HPE GreenLake/DHCP). It also disconnects any active connection to the HPE Aruba Networking Central server.

Example

```
switch(config-hpe-anw-central) # disable
switch(config-hpe-anw-central) #
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-hpe_anw-central	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables connection to HPE Aruba Networking Central server. When the connection is enabled, the switch attempts to download the location of the HPE Aruba Networking Central server in one of the following ways at startup and after the connection is lost:

- Using command-line interface (CLI).
- Connecting to the HPE GreenLake server.
- Using DHCP options provided during ZTP.

DHCP servers provide the options requested by the device to connect to Central, Central On-premise management, or the TFTP server.



When a switch is able to connect to HPE Aruba Networking Central, but is not registered in the HPE Aruba Networking Central inventory or does not have a proper license, the switch will get disconnected. If the HPE Aruba Networking Central feature is enabled using this command, the switch will then reconnect back to HPE Aruba Networking Central and will get disconnected again. This connect/disconnect process will continue until the switch is properly registered in HPE Aruba Networking Central. To avoid this unnecessary reconnection cycle, best practices is to [disable HPE Aruba Networking Central](#) until the switch is registered in HPE Aruba Networking Central, or a license is obtained for that device.

Examples

```
switch(config-hpe-anw-central) # enable
switch(config-hpe-anw-central) #
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-hpe_anw-central	Administrators or local user group members with execution rights for this command.

location-override

```
location-override <location> [vrf <VRF-NAME>]
no location-override
```

Description

When **location** and **vrf** are configured, the switch overrides existing connections to HPE Aruba Networking Central. The switch attempts to establish connection to HPE Aruba Networking Central with the specified location and VRF with highest priority.

Location can take one of the following values:

- A fully qualified domain name (FQDN) along with an optional port number.
- An IPv4 address with an optional port number.
- An IPv6 address with an optional port number.

If the port number is not specified, then port 443 is used by default. If the command is executed without the VRF parameter, the switch uses the 'default' VRF.

The **no** form of this command removes location override values from the HPE Aruba Networking Central configuration context.



When you configure an IPv6 address with a port number, specify the address part inside square brackets, optionally followed by the port number, e.g. [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443.

Parameter	Description
<code><location></code>	Specifies one of these values: ▪ <code><FQDN></code>: a fully qualified domain name. ▪ <code><IPv4></code>: an IPv4 address. ▪ <code><IPv6></code>: an IPv6 address.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Examples

Configuring location override with location and VRF:

```
switch(config-hpe-anw-central)# location-override hpe-anw-central.com vrf default
switch(config-hpe-anw-central)#
switch(config-hpe-anw-central)# location-override hpe-anw-central.com vrf red
switch(config-hpe-anw-central)# location-override 10.0.0.1 vrf red
switch(config-hpe-anw-central)# location-override 10.0.0.1:443 vrf red
switch(config-hpe-anw-central)# location-override
2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf red
switch(config-hpe-anw-central)# location-override
[2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443 vrf red
```

Configuring location override with location only:

```
switch(config-hpe-anw-central)# location-override hpe-anw-central.com
switch(config-hpe-anw-central)#
```

Removing location override values from the HPE Aruba Networking Central configuration context:

```
switch(config-hpe-anw-central)# no location-override
switch(config-hpe-anw-central)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.13.1000	Command updated to reflect an OTP scenario.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-hpe_anw-central	Administrators or local user group members with execution rights for this command.

location-override-alternative

```
location-override-alternative <LOCATION> [vrf <VRF>]  
no location-override-alternative <LOCATION> [vrf <VRF>]
```

Description

Configures information about HPE Aruba Networking Central connection when the alternative location is used.

The **no** form of this command removes the **location-override-alternative** configuration.

Parameter	Description
<LOCATION>	Specifies the HPE Aruba Networking Central location.
vrf <VRF>	Specifies the VRF used to connect to HPE Aruba Networking Central.

Usage

When the main and alternative HPE Aruba Networking Central server locations are specified, the switch attempts to connect to the main HPE Aruba Networking Central server. If there is connectivity failure with the main HPE Aruba Networking Central server location, it attempts to establish a connection with the alternative server location.

If the alternative location is configured without a main location, the user is prompted for confirmation. In this case, there is no redundancy and the switch attempts to connect to the alternative location.

Location can take one of the following values:

- A fully qualified domain name (FQDN) along with an optional port number.
- An IPv4 address with an optional port number.
- An IPv6 address with an optional port number.

If the port number is not specified, then port 443 is used by default. If the command is executed without the VRF parameter, the switch uses the 'default' VRF.

An HPE Aruba Networking Central server location can only be a fully qualified domain name (FQDN) or a valid IP address. If the command is entered without the VRF parameter, the switch uses the default VRF.

Examples

Example of configuring with the hpe-anw-central.com location and VRF red:

```
switch(config-hpe-anw-central)# location-override-alternative hpe-anw-central.com vrf red
switch(config-hpe-anw-central)#
```

Example of a configuration with location only:

```
switch(config-hpe-anw-central)# location-override-alternative hpe-anw-central.com
switch(config-hpe-anw-central)#
```

Example of removing the override configuration:

```
switch(config-hpe-anw-central)# no location-override-alternative
switch(config-hpe-anw-central)# location-override-alternative 10.0.0.1 vrf red
switch(config-hpe-anw-central)# location-override-alternative 10.0.0.1:443 vrf red
switch(config-hpe-anw-central)# location-override-alternative 2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf red
switch(config-hpe-anw-central)# location-override-alternative [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443 vrf red
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.13.1000	Command updated to reflect OTP scenario.
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-hpe_anw-central	Administrators or local user group members with execution rights for this command.

show hpe-anw-central

```
show hpe-anw-central
```

Description

Shows information about HPE Aruba Networking Central connection and the status of the Activate server connection.

Examples

Example of a switch that has the HPE Aruba Networking Central connection:

```
switch# show hpe-anw-central
Central admin state           : enabled
Central location              : 10.0.0.1
VRF for connection            : mgmt
Shared Token                   : N/A
Central connection status     : connected
Central source                 : activate
Central source connection status : connected
Central source last connected on : Wed Jun 28 23:07:25 UTC 2023
Main location                  : 10.0.0.1
Main VRF                       : mgmt
Alternative location           : N/A
Alternative VRF                : N/A
Activate Server URL             : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                      : N/A
Source IP Overridden           : False
Central support mode           : disabled
```

Example of a switch when the main CLI location is used:

```
switch# show hpe-anw-central
Central admin state           : enabled
Central location              : 10.0.0.1
VRF for connection            : mgmt
Shared secret                  : N/A
Central connection status     : connected
Central source                 : cli
Central source connection status : connected
Central source last connected on : Wed Jun 28 23:07:25 UTC 2023
Main location                  : 10.0.0.1
Main VRF                       : mgmt
Alternative location           : 20.0.0.1
Alternative VRF                : N/A
Activate server URL             : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                      : N/A
Source IP Overridden           : False
Central support mode           : disabled
```

Example of a switch when the alternative CLI location is used:

```
switch# show hpe-anw-central
Central admin state           : enabled
Central location              : 20.0.0.1
VRF for connection            : default
Shared secret                  : N/A
Central connection status     : connected
Central source                 : cli
Central source connection status : connected
```

```

Central source last connected on      : Wed Jun 28 23:07:25 UTC 2023
Main location                        : 10.0.0.1
Main VRF                            : mgmt
Alternative location                 : 20.0.0.1
Alternative VRF                      : default
Activate server URL                  : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                           : N/A
Source IP Overridden                 : False
Central support mode                 : disabled
Central admin state                   : enabled
Central location                     : 20.0.0.1
VRF for connection                   : default
Shared secret                        : N/A
Central connection status             : connected
Central source                       : cli
Central source connection status      : connected
Central source last connected on      : Wed Jun 28 23:07:25 UTC 2023
Main location                        : 10.0.0.1
Main VRF                            : mgmt
Alternative location                 : 20.0.0.1
Alternative VRF                      : N/A
Activate server URL                  : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                           : N/A
Source IP Overridden                 : False
Central support mode                 : disabled

```

Example of a switch when the location is obtained from DHCP options:

```

switch# show hpe-anw-central
Central admin state                   : enabled
Central location                     : central-western-us.arubanetworks.com
VRF for connection                   : mgmt
Shared secret                        : N/A
Central connection status             : connected
Central source                       : DHCP
Central source connection status      : connected
Central source last connected on      : Fri Jun 30 20:22:33 UTC 2023
Main location                        : central-western-us.arubanetworks.com
Main VRF                            : mgmt
Alternative location                 : N/A
Alternative VRF                      : N/A
Activate server URL                  : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                           : 100.0.0.1
Source IP Overridden                 : False
Central support mode                 : disabled

```

Example of a switch when HPE Aruba Networking Central is disabled:

```

switch# show hpe-anw-central
Central admin state                   : disabled
Central location                     : N/A
VRF for connection                   : N/A
Shared secret                        : N/A
Central connection status             : N/A
Central source                       : none
Central source connection status      : N/A

```

```

Central source last connected on      : N/A
Main location                        : N/A
Main VRF                            : N/A
Alternative location                 : N/A
Alternative VRF                     : N/A
Activate server URL                  : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                           : N/A
Source IP Overridden                 : False
Central support mode                 : disabled
Central admin state                  : disabled
Central location                    : N/A
VRF for connection                  : N/A
Shared secret                       : N/A
Central connection status            : N/A
Central source                      : none
Central source connection status     : N/A
Central source last connected on     : N/A
Main location                        : N/A
Main VRF                            : N/A
Alternative location                 : N/A
Alternative VRF                     : N/A
Activate server URL                  : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                           : N/A
Source IP Overridden                 : False
Central support mode                 : disabled

```

Example of a switch when HPE Aruba Networking Central is not reachable:

```

switch# show hpe-anw-central
Central admin state      : enabled
Central location        : N/A
VRF for connection      : N/A
Shared secret           : N/A
Central connection status : not-reachable
Central source          : activate
Central source connection status : connected
Central source last connected on : Fri Jun 30 20:22:33 UTC 2023
Main location           : N/A
Main VRF                : N/A
Alternative location     : N/A
Alternative VRF         : N/A
Activate server URL      : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP               : N/A
Source IP Overridden     : False
Central support mode     : disabled

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.15	Command syntax changed from aruba-central to hpe-anw-

Release	Modification
	central.
10.12.1000	Enhanced to support more scenarios
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show running-config current-context

show running-config current-context

Description

Shows the running configuration for the current-context. If user is in the context of HPE Aruba Networking Central (**config-hpe-anw-central**), then the HPE Aruba Networking Central running configuration is displayed.

Examples

Shows the running configuration of HPE Aruba Networking Central:

```
switch(config-hpe-anw-central)# show running-config current-context
hpe-anw-central
disable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

banner

```
banner {motd | exec} <DELIMITER>
no banner {motd | exec} <DELIMITER>
```

Description

Enables the customization of the MOTD or the EXEC banner.
The **no** form of this command disables the MOTD or the EXEC banner.

Command context

config

Parameter	Description
motd	Configures the banner shown before the login prompt.
exec	Configures the banner shown after a successful login.
<DELIMITER>	Specifies the character used to terminate the input string.

Authority

Administrators or local user group members with execution rights for this command.

Usage

This command enables the customization of two types of banners:

- The MOTD banner. The banner displayed on attempting to connect to a management interface.
- The EXEC banner. The banner displayed upon successful authentication.

You can create a banner that spans multiple lines. The maximum length of a banner is 4,095 characters. This requirement includes any non-visible characters. The minimum number of characters allowed is an empty string, which displays no banner.

End the banner text with a chosen delimiter character. A delimiter character can be any non-whitespace character that does not have special meaning to the CLI, such as the caret (^). A question mark (?) is not permitted. Question marks can however be included as part of the banner text.

Examples

Configuring the banner displayed before login:

```
switch(config)# banner motd ^
Enter a new banner. Terminate the banner with the delimiter you have chosen.
(banner-motd)# This is an example of a banner text which a connecting user
```



```
(banner-motd) # will see before they are prompted for their password.  
(banner-motd) #  
(banner-motd) # As you can see it may span multiple lines and the input  
(banner-motd) # will be terminated when the delimiter character is  
(banner-motd) # encountered.^
```

Configuring the banner displayed after a successful login:

```
switch(config) # banner exec &  
Enter a new banner. Terminate the banner with the delimiter you have chosen.  
(banner-motd) # This is an example of different banner text. This time  
(banner-motd) # the banner entered will be displayed after a user has  
(banner-motd) # authenticated.  
(banner-motd) #  
(banner-motd) # & This text will not be included because it comes after the &
```

Disabling the MOTD banner:

```
switch(config) # no banner motd ^
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show banner

```
show banner {motd | exec} [vsx-peer]
```

Description

Shows the MOTD or EXEC banner message.

Parameter	Description
motd	Shows the banner displayed before the login prompt.
exec	Shows the banner displayed after a successful login.
[vsx-peer]	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the MOTD banner displayed before the login prompt:

```
switch(config)# show banner motd
This is an example of a banner text which a connecting user
will see before they are prompted for their password.

As you can see it may span multiple lines and the input
will be terminated when the delimiter character is
encountered.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

bfd

bfd
no bfd

Description

Enables BFD support on the switch. BFD is disabled by default.

The **no** form of this command disables BFD and removes all related configuration settings. To disable BFD, but retain configuration settings, use the command [bfd disable](#).

Examples

Enabling BFD support:

```
switch(config)# bfd
```

Disabling BFD support and removing all configuration settings:

```
switch(config)# no bfd
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

bfd <IPV4-ADDR>

bfd <IPV4-ADDR>
no bfd <IPV4-ADDR>

Description

Enables BFD under VRRP for the specified IP address. BFD is asynchronous and echo mode is supported.

The **no** form of this command disables BFD under VRRP for the specified IP address.

Parameter	Description
<code><IPV4-ADDR></code>	Specifies the address on which to enable BFD in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Enabling BFD on the address **10.0.0.1** on VRRP **1**:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# bfd 10.0.0.1
```

Disabling BFD on the address **10.0.0.1** on VRRP **1**:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# no bfd 10.0.0.1
```



For more information on features that use this command, refer to the High Availability Guide or IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vrrp	Administrators or local user group members with execution rights for this command.

bfd all-interfaces

```
bfd all-interfaces
no bfd all-interfaces
```

Description

Enables BFD on all OSPFv2 or OSPFv3 interfaces.

The **no** form of this command disables BFD on all active OSPFv2/OSPFv3 or IPv4/IPv6 interfaces, excluding those on which BFD was enabled at the interface level with the commands `ip ospf bfd` and `ipv6 ospfv3 bfd`.

Examples

Enabling BFD on all OSPFv2 interfaces:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# bfd all-interfaces
```

Disabling BFD on all OSPFv2 interfaces:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# no bfd all-interfaces
```

Enabling BFD on all OSPFv3 interfaces:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# bfd all-interfaces
```

Disabling BFD on all OSPFv3 interfaces:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no bfd all-interfaces
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf- <i><INSTANCE-TAG></i> config-ospfv3- <i><INSTANCE-TAG></i>	Administrators or local user group members with execution rights for this command.

bfd detect-multiplier

```
bfd detect-multiplier <MULTIPLIER>  
no bfd detect-multiplier <MULTIPLIER>
```

Description

Sets BFD detection multiplier on an interface.

The **no** form of this command removes the configured BFD detection multiplier.

Parameter	Description
<code><MULTIPLIER></code>	Specifies the BFD detection multiplier. Range: 1 to 5. Default: 5.

Examples

Setting the BFD detection multiplier to **3**:

```
switch(config-if)# bfd detect-multiplier 3
```

Removing the BFD detection multiplier:

```
switch(config-if)# no bfd detect-multiplier 3
```

Setting the BFD detection multiplier to the default value:

```
switch(config-if)# no bfd detect-multiplier
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

bfd disable

bfd disable

Description

Disables BFD on the switch, but retains all configuration settings.

Examples

Disabling BFD:

```
switch(config)# bfd disable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

bfd enable (Context: config-hsc)

```
switch(config-hsc)# bfd enable
switch(config-hsc)# no bfd enable
```

Description

Enables or disables BFD for HSC feature.

Usage

BFD must be enabled globally to work for HSC.

Examples

Enabling BFD support for HSC:

```
switch(config)# hsc
switch(config-hsc)# bfd enable
```

Disabling BFD support for HSC:

```
switch(config)# hsc
switch(config-hsc)# no bfd enable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

bfd disable (Context: config-hsc)

```
switch(config-hsc)# bfd disable
```

Description

Disables BFD for HSC feature.

Example

Disabling BFD support for HSC:

```
switch(config)# hsc  
switch(config-hsc)# bfd disable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

bfd echo disable

```
bfd echo disable  
no bfd echo disable
```

Description

Disables support for BFD echo packets. Echo packet support is enabled by default.

The **no** form of this command enables support for BFD echo packets.



Toggling this feature on 8100, 8325, 8360, 9300, 9300S switches may cause route flapping.



BFD IPv6 Echo is not supported.

Authority

Examples

Enabling BFD echo packet support on all interfaces:

```
switch(config)# no bfd echo disable
```

Disabling BFD echo packet support on all interfaces:

```
switch(config)# bfd echo disable
```

Enabling BFD echo packet support on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# bfd echo disable
```

Disabling BFD echo packet support on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no bfd echo disable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config config-if	Administrators or local user group members with execution rights for this command.

bfd min-echo-receive-interval

```
bfd min-echo-receive-interval <INTERVAL>
no bfd min-echo-receive-interval <INTERVAL>
```

Description

Sets the minimum time interval between received BFD echo packets.

The **no** form of this command removes the configured BFD echo packets interval. If the interval is not set, the default interval is used.



BFD IPv6 Echo is not supported.

Parameter	Description
<code><INTERVAL></code>	Specifies the minimum reception interval in milliseconds. A value of 0 means that the switch does not support reception of BFD echo packets. Range: 0, 50 to 1000. Default: 500.

Examples

Setting the minimum reception interval to **1000** milliseconds:

```
switch(config)# bfd min-echo-receive-interval 1000
```

Removing the minimum reception interval:

```
switch(config)# no bfd min-echo-receive-interval 1000
```

Setting the minimum reception interval to the default value:

```
switch(config)# no bfd min-echo-receive-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

bfd min-receive-interval

```
bfd min-receive-interval <INTERVAL>  
no bfd min-receive-interval <INTERVAL>
```

Description

Sets the minimum time interval between received BFD control packets on an interface.

The **no** form of this command removes the configured BFD minimum interval on an interface. If the interval is not set, the default interval is used.

Parameter	Description
<code><INTERVAL></code>	Specifies the minimum receive interval in milliseconds. A value of 0 means that the switch does not support reception of BFD control packets. Range: 100 to 20000. Default: 3000.

Examples

Setting the minimum receive interval to **1000** milliseconds:

```
switch(config-if)# bfd min-receive-interval 1000
```

Removing the minimum receive interval:

```
switch(config-if)# no bfd min-receive-interval 1000
```

Setting the minimum receive interval to the default value:

```
switch(config-if)# no bfd min-receive-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

bfd min-transmit-interval

```
bfd min-transmit-interval <INTERVAL>  
no bfd min-transmit-interval <INTERVAL>
```

Description

Sets the minimum time interval between transmitted BFD control packets on an interface.

The **no** form of this command removes the configured BFD minimum transmitted interval on an interface. If the interval is not set, the default interval is used.

Parameter	Description
<INTERVAL>	Specifies the minimum transmit interval in milliseconds. Range: 50 to 20000 (8320, 8325, 9300/9300S). Default: 3000.

Usage

- If the minimum time interval is set between 500 ms and 1000 ms, then **bfd detect-multiplier** must be set to at least 3.
- If **bfd detect-multiplier** is set to 1, then the minimum transmit interval must be set to at least 3000 ms.
- Whenever the minimum time interval is set to a value less than 1000 ms, BFD automatically adjusts the transmission interval to 1000 ms if any of the following conditions apply:
 - The session is operating in asynchronous mode and echo is enabled.
 - The session state is in any other state than **up**.

As described in RFC 5880, this behavior occurs because BFD echo provides quick detection which allows the BFD asynchronous session to lower its traffic/resource requirements.



BFD IPv6 Echo is not supported.

Examples

Setting the minimum transmit interval to **500** ms:

```
switch(config-if) # bfd min-transmit-interval 500
```

Removing the minimum transmit interval:

```
switch(config-if) # no bfd min-transmit-interval 500
```

Setting the minimum transmit interval to the default value:

```
switch(config-if) # no bfd min-transmit-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

clear bfd statistics

```
clear bfd statistics [session <ID>]
```

Description

Clears statistics for all BFD sessions or for a specific BFD session.

Parameter	Description
session <ID>	Specifies a session ID.

Examples

Clearing statistics for all BFD sessions:

```
switch# clear bfd statistics
```

Clearing statistics for BFD session 1:

```
switch# clear bfd statistics session 1
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

ip ospf bfd

```
ip ospf bfd
no ip ospf bfd
```

Description

Enables BFD for OSPFv2 on the current interface. The interface must have OSPFv2 enabled on it. This overrides the global settings defined with the command **bfd all-interfaces**.

The **no** form of this command sets the current interface to the global settings defined with the command **bfd all-interfaces**.

Examples

Enabling BFD on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf bfd
```

Disabling BFD on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip ospf bfd
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip ospf bfd disable

ip ospf bfd disable

Description

Disables BFD for OSPFv2 on the current interface. This overrides the global settings defined with the command **bfd all-interfaces**.

Examples

Enabling BFD on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf bfd disable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip route bfd

```
ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR> | <INTERFACE> | nullroute |  
reject]  
    {bfd | distance | name | tag | track | use-forwarding-address | vrf}  
no ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR> | <INTERFACE> | nullroute |  
reject]  
    {bfd | distance | name | tag | track | use-forwarding-address | vrf}
```

Description

Enables or disables BFD on the specified static route. To disable BFD, issue the command without the `bfd` option.

Parameter	Description
<DEST-IPV4-ADDR>	Specifies a route destination in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<NETMASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<NEXT-HOP-IP-ADDR>	Specifies the next hop address for reaching the destination in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<INTERFACE>	Specifies the next hop as an outgoing interface.
bfd	Enables BFD on the static route. Omit this parameter to disable BFD.
name <WORD>	Assigns a name to the destination route. Range: 1 to 64 characters.
tag <1-4294967295>	Specifies and assigns tag for the route.
vrf <DST-VRF-NAME>	The VRF route leak destination.

Examples

Enabling BFD on a static route:

```
switch(config)# interface 1/1/1
switch(config-if)# ip address 20.1.1.2/24
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip route 192.0.0.0/8 20.1.1.1 bfd
switch(config)# ip route 1.1.2.0 255.255.255.0 2.2.2.2 bfd name AdminRoute
```

Disabling BFD on a static route:

```
switch(config)# ip route 192.0.0.0/8 20.1.1.1
```



For more information on features that use this command, refer to the High Availability Guide or IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	The name parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 bfd

```
ipv6 ospfv3 bfd
no ipv6 ospfv3 bfd
```

Description

Enables BFD for OSPFv3 on the current interface. The interface must have OSPFv3 enabled on it. This overrides the global settings defined with the command **bfd all-interfaces**.

The **no** form of this command sets the current interface to the global settings defined with the command **bfd all-interfaces**.

Examples

Enabling BFD:

```
switch(config-if)# ipv6 ospfv3 bfd
```

Disabling BFD:


```
switch(config-if)# no ipv6 ospfv3 bfd
```

Enabling BFD on a subinterface:

```
switch(config-subif)# ipv6 ospfv3 bfd
```

Disabling BFD on a subinterface:

```
switch(config-subif)# no ipv6 ospfv3 bfd
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.14	Support added for the 9300 and 9300S switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 bfd disable

ipv6 ospfv3 bfd disable

Description

Disables BFD on the current OSPFv3 interface. This overrides the global settings defined with the command `bfd all-interfaces`.

Examples

Enabling BFD on interface 1/1/1 :

```
switch(config)# interface 1/1/1  
switch(config-if)# ipv6 ospfv3 bfd disable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.14	Support added for the 9300 and 9300S switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

neighbor fall-over bfd

```
neighbor {<IP-ADDRESS>|<PEER-GROUP-NAME>} fall-over bfd
no neighbor {<IP-ADDRESS>|<PEER-GROUP-NAME>} fall-over bfd
```

Description

Enables BGP to register with BFD to receive fast peering session deactivation messages from BFD. The **no** form of this command disables BGP for BFD.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<PEER-GROUP-NAME>	Specifies a peer group.

Examples

```
switch(config-router)# neighbor 1.1.1.1 fall-over
switch(config-router)# no neighbor 1.1.1.1 fall-over bfd
```

```
switch(config-router)# neighbor PG fall-over
switch(config-router)# no neighbor PG fall-over bfd
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.14	Support added for the 9300 and 9300S switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 bfd

```
ospfv3-af ipv4 bfd
no ospfv3-af ipv4 bfd
```

Description

Enables BFD for OSPFv3 AF on the current interface. The interface must have OSPFv3 AF enabled on it. The **no** form of this command disables BFD on the current interface.



OSPFv3 AF IPv4 sessions are established through the IPv6 link-local address. Therefore, a BFD session is also created for the IPv6 link-local address to monitor the path and establish neighborship.

Examples

Enabling BFD:

```
switch(config-if) # ospfv3-af ipv4 bfd
```

Disabling BFD:

```
switch(config-if) # no ospfv3-af ipv4 bfd
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 bfd

```
ospfv3-af ipv6 bfd
no ospfv3-af ipv6 bfd
```

Description

Enables BFD for OSPFv3 AF on the current interface. The interface must have OSPFv3 AF enabled on it. The **no** form of this command disables BFD on the current interface.

Examples

Enabling BFD:

```
switch(config-if)# ospfv3-af ipv6 bfd
```

Disabling BFD:

```
switch(config-if)# no ospfv3-af ipv6 bfd
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

show bfd

```
show bfd [session <ID>] [all-vrfs | vrf <NAME>] [vsx-peer]
```

Description

Shows information for all BFD sessions or for a specific BFD session.

Parameter	Description
session <ID>	Session ID.
all-vrfs	All VRFs.
vrf <NAME>	Specifies the name of a VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Possible values for **State** are:

- Up
- Down
- AdminDown
- Init

Possible values for **Local diagnostic** and **Remote diagnostic** are:

- Control detection time expired (1): The session has stopped receiving BFD control packets from the peer after one detection time.
- Echo function failed: The session has stopped receiving BFD Echo packets, so the session was declared Down.
- Neighbor signaled session down: A packet from the peer was received with either AdminDown or Down state.
- Forwarding plane reset: Not set in this release.
- Path down: The forwarding path when Down.
- Concatenated path down: Not set in this release.
- Administratively down: The administrator has disabled BFD.
- Reverse concatenated path down: Not set in this release.



BFD IPv6 Echo is not supported.

Examples

Showing information for all BFD sessions:

```
switch# show bfd
```

```
Admin status : Enabled
Echo source IP : 2.2.2.2
Statistics:
```

```
Total Number of Control Packets Transmitted : 42
Total Number of Control Packets Received : 42
Total Number of Control Packets Dropped : 0
```

Session	Interface	VRF	Source IP	Destination IP
	Echo	State	Application	
1	vlan10	blue	10.10.10.1	10.10.10.2
	disabled	up	ospf	
1	vlan10	blue	N/A	10.10.10.2
	disabled	up	static_routes	
2	vlan40	red	40.10.10.1	40.10.10.2
	disabled	up	ospf	
3	vlan30	red	30.10.10.1	30.10.10.2
	disabled	up	ospf	
4	vlan20	blue	20.10.10.1	20.10.10.2
	disabled	up	ospf	
5	vlan50	black	50.10.10.1	50.10.10.2
	disabled	up	ospf	
6	vlan60	black	60.10.10.1	60.10.10.2

```

        disabled up      ospf
7      vlan10    blue    fe80::409:7380:a62:2400
fe80::409:7380:a49:a200      disabled up      ospfv3

```

```

Admin status : Enabled
Echo source IP : 2.2.2.2
Statistics:
Total Number of Control Packets Transmitted : 42
Total Number of Control Packets Received : 42
Total Number of Control Packets Dropped : 0

```

Session	Interface	VRF	Source IP	Destination IP
	Echo	State	Application	
1	vlan10	blue	10.10.10.1	10.10.10.2
	disabled	up	ospf	
1	vlan10	blue	N/A	10.10.10.2
	disabled	up	static_routes	
2	vlan40	red	40.10.10.1	40.10.10.2
	disabled	up	ospf	
3	vlan30	red	30.10.10.1	30.10.10.2
	disabled	up	ospf	
4	vlan20	blue	20.10.10.1	20.10.10.2
	disabled	up	ospf	
5	vlan50	black	50.10.10.1	50.10.10.2
	disabled	up	ospf	
6	vlan60	black	60.10.10.1	60.10.10.2
	disabled	up	ospf	
7	vlan10	blue	fe80::409:7380:a62:2400	
	fe80::409:7380:a49:a200	disabled	up	ospfv3

Showing information for BFD session 1:

```

switch# show bfd session 1
BFD Session Information - Session 1
VRF: blue
Min Tx Interval (msec) : 10000
Min Rx Interval (msec) : 10000
Min Echo Rx Interval (msec) : 700
Detect Multiplier : 3
Application : ospf
Local Discriminator : 1
Remote Discriminator : 1
Echo : Enabled
Local Diagnostic : no_diagnostic
Remote Diagnostic: administratively_down
State flaps: 0

```

Interface	Source IP	Destination IP	State	Pkt In	Pkt Out	Pkt Drop
1/1/1	100.100.100.100	100.100.100.101	Up	100	101	0

```

BFD Session Information - Session 1
VRF: blue
Min Tx Interval (msec) : 10000
Min Rx Interval (msec) : 10000
Min Echo Rx Interval (msec) : 700
Detect Multiplier : 3
Application : ospf
Local Discriminator : 1
Remote Discriminator : 1
Echo : Enabled

```

```

Local Diagnostic : no_diagnostic
Remote Diagnostic: administratively_down
State flaps: 0
Interface Source IP      Destination IP  State      Pkt In   Pkt Out   Pkt Drop
-----
1/1/1      100.100.100.100 100.100.100.101 Up          100       101        0

```

Showing information for all BFD sessions related to a particular VRF in the system:

```

switch# show bfd vrf blue

Admin status: enabled
Echo source IP: 100.1.1.1
Statistics:
Total number of control packets transmitted: 2226
Total number of control packets received: 2222
Total number of control packets dropped: 0
Session Interface VRF      Source IP      Destination IP
      Echo      State      Application
-----
1      vlan10    blue      10.10.10.1      10.10.10.2
      disabled up      ospf
1      vlan10    blue      N/A              10.10.10.2
      disabled up      static_routes
4      vlan20    blue      20.10.10.1      20.10.10.2
      disabled up      ospf
7      vlan10    blue      fe80::409:7380:a62:2400
fe80::409:7380:a49:a200      disabled up      ospfv3

```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show bfd interface

```
show bfd interface <NAME>
```

Description

Shows information for all BFD sessions related to the specified interface.

Parameter	Description
interface <NAME>	Specifies an interface.



BFD IPv6 Echo is not supported.

Examples

Showing information for all BFD sessions related to the specified interface:

```
switch# show bfd interface vlan10

BFD session information - Session 1
Min Tx interval (msec): 3000
Min Rx interval (msec): 3000
Min echo Rx interval (msec): 500
Detect multiplier: 5
Application: ospf
Local discriminator: 13211
Remote discriminator: 13211
Echo: disabled
Local diagnostic: no_diagnostic
Remote diagnostic: no_diagnostic
State flaps: 0
Interface Source IP          Destination IP
      State      Pkt Rx    Pkt Tx    Pkt drop
-----
vlan10  10.10.10.1          10.10.10.2
      up          453      455      0

=====
BFD session information - Session 1
Min Tx interval (msec): 3000
Min Rx interval (msec): 3000
Min echo Rx interval (msec): 500
Detect multiplier: 5
Application: static_routes
Local discriminator: 13211
Remote discriminator: 13211
Echo: disabled
Local diagnostic: no_diagnostic
Remote diagnostic: no_diagnostic
State flaps: 0
Interface Source IP          Destination IP
      State      Pkt Rx    Pkt Tx    Pkt drop
-----
vlan10  N/A              10.10.10.2
      up          453      455      0

=====
BFD session information - Session 7
Min Tx interval (msec): 3000
Min Rx interval (msec): 3000
Min echo Rx interval (msec): 500
Detect multiplier: 5
Application: ospfv3
Local discriminator: 1402
```



```

Remote discriminator: 1402
Echo: disabled
Local diagnostic: no_diagnostic
Remote diagnostic: no_diagnostic
State flaps: 0
Interface Source IP          Destination IP
      State      Pkt Rx    Pkt Tx    Pkt drop
-----
vlan10  fe80::409:7380:a62:2400  fe80::409:7380:a49:a200
      up          58        58        0

```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show hsc

show hsc

Description

Displays connection information for the remote controller.

Example

Displaying connection information for the remote controller:

```

switch# show hsc

BFD status : Enabled

Controller IP   Port   Connection status  Connection state
-----
192.168.16.17  6640   UP                ACTIVE
192.168.16.17  6650   UP                IDLE
192.168.16.17  6660   DOWN             BACKOFF

```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

address-family

```
address-family {{ipv4 | ipv6} unicast | l2vpn evpn}
no address-family {{ipv4 | ipv6} unicast | l2vpn evpn}
```

Description

Specifies address family to use and changes to the configuration context for the specified family:

- **config-bgp-ipv4-uc** for IPv4 unicast
- **config-bgp-ipv6-uc** for IPv6 unicast
- **config-bgp-l2vpn-evpn** for L2VPN EVPN

The **no** form of this command removes the specified address family configuration.

Parameter	Description
ipv4	Selects the IPv4 address family.
ipv6	Selects the IPv6 address family.
unicast	Specifies unicast addresses.
l2vpn evpn	Selects the L2VPN EVPN address family. Route maps with the match vni clause can be used with L2VPN EVPN neighbors only.

Example

Setting the address family to IPv4 unicast.

```
switch(config-bgp) # address-family ipv4 unicast
switch(config-bgp-ipv4-uc) #
```

Setting the address family to L2VPN EVPN.

```
switch(config-bgp) # address-family l2vpn evpn
switch(config-bgp-l2vpn-evpn) #
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

aggregate-address

```
aggregate-address <IP-ADDR>/<MASK> [as-set] [summary-only]
[suppress-map <MAP-NAME>] [advertise-map <MAP-NAME>]
[attribute-map <MAP-NAME>]
```

```
no aggregate-address <IP-ADDR>/<MASK> [as-set] [summary-only]
[suppress-map <MAP-NAME>] [advertise-map <MAP-NAME>]
[attribute-map <MAP-NAME>]
```

```
[no] aggregate-address split-horizon
```

Description

Creates an aggregate address entry in the BGP routing table.

The **no** form of this command removes the specified aggregate address entry.

Parameter	Description
<ADDRESS>	Specifies an aggregate address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx), where x is a hexadecimal number from 0 to F.
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
as-set	The AS_PATH attribute advertised for this route will contain an AS_SET consisting of all AS numbers contained in all paths that are being summarized.
summary-only	Creates the aggregate route but also suppresses advertisements of more-specific routes to all neighbors.
suppress-map <MAP-NAME>	Specifies an aggregate route for creation, but suppresses the advertisement of the created route. Match clauses of route maps can be used to suppress some more-specific routes of the aggregate selectively, and leave others unsuppressed. IP prefix lists and as_path lists match clauses are supported.
advertise-map <MAP-NAME>	Specifies routes that will be used to build attributes of the aggregate route, such as AS_SET or community.
attribute-map <MAP-NAME>	Specifies that the attributes of the aggregate route can be changed.

Examples

```
switch(config-bgp-ipv4-uc) # aggregate-address 10.0.0.0/8
switch(config-bgp-ipv4-uc) # no aggregate-address 10.0.0.0/8
```

```
switch(config-bgp-ipv6-uc) # aggregate-address 2001:0db8:85a3::8a2e:0370:7334/24
switch(config-bgp-ipv6-uc) # no aggregate-address 2001:0db8:85a3::8a2e:0370:7334/24
```

```
switch(config-bgp-ipv4-uc) # aggregate-address 10.0.0.0/8 as-set summary-only
switch(config-bgp-ipv4-uc) # aggregate-address 10.0.0.0/8 attribute-map RMap
```

```
switch(config-bgp-ipv6-uc) # aggregate-address 2001:0db8:85a3::8a2e:0370:7334/24
as-set summary-only
switch(config-bgp-ipv6-uc) # aggregate-address 2001:0db8:85a3::8a2e:0370:7334/24
attribute-map RMap
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

bgp add-paths select best 2

```
bgp add-paths select best 2
no bgp add-paths select best 2
```

Description

Enables BGP-PIC and is available in the router BGP context.
The **no** form of this command disables BGP-PIC.

Parameter	Description
additional-paths	Specifies the number of paths.

Usage

- When BGP-PIC is enabled or disabled, there will be a momentary traffic loss for a few seconds due to all BGP routes being potentially deleted and re-added as necessary.
- Two paths are required for protected routes.

Examples

Enabling BGP-PIC:

```
switch(config)# router bgp 1
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# bgp add-paths select best 2
switch(config-bgp-ipv4-uc)#
^^^
```

Disabling BGP-PIC:

```
switch(config)# router bgp 1
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# no bgp add-paths select best 2
switch(config-bgp-ipv4-uc)#
^^^
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14.1000 or later	Command introduced on 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp always-compare-med

```
bgp always-compare-med
no bgp always-compare-med
```

Description

Enables comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command sets comparison of MED to the default setting (disabled).

Usage

- MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.
- During the best-path selection process, MED comparison is done only among paths from the same autonomous system. Use the command `bgp always-compare-med` to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

Examples

```
switch(config-bgp)# bgp always-compare-med  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp always-compare-med  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp asnotation dotted

```
bgp asnotation dotted  
no bgp asnotation dotted
```

Description

Specifies that Autonomous System (AS) numbers greater than 65535 be shown in dotted integer format for all show commands, including running-configuration.

The **no** form of this command restores the default format of non-dotted, simple integer.

Example

```
switch(config-bgp)# bgp asnotation dotted
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp asnotation dotted-plus

bgp asnotation dotted-plus
no bgp asnotation dotted-plus

Description

Specifies that all Autonomous System (AS) numbers be shown in dotted integer format for all show commands, including running-configuration.

The **no** form of this command restores the default format of non-dotted, simple integer.

Example

```
switch(config-bgp)# bgp asnotation dotted-plus
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp bestpath as-path ignore

bgp bestpath as-path ignore
no bgp bestpath as-path ignore

Description

Configures BGP to avoid considering the autonomous system (AS) path during best path route selection. By default, the AS-path is considered during BGP best path selection.

Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command restores default behavior which configures BGP to consider the AS-path during route selection.

Examples

```
switch(config-bgp)# bgp bestpath as-path ignore  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp bestpath as-path ignore  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp bestpath as-path multipath-relax

```
bgp bestpath as-path multipath-relax  
no bgp bestpath as-path multipath-relax
```

Description

Configures Border Gateway Protocol (BGP) to treat two BGP routes as equal cost even if their AS-paths differ, as long as their AS-path lengths and other relevant attributes are the same. This allows routes with different AS-paths to be programmed into the forwarding table as equal cost multipath routes.

Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command restores the default behavior which configures BGP to treat two BGP routes as different costs when their AS-paths differ.

Examples

```
switch(config-bgp)# bgp bestpath as-path multipath-relax  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp bestpath as-path multipath-relax  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp bestpath compare-routerid

```
bgp bestpath compare-routerid  
no bgp bestpath compare-routerid
```

Description

Configures a BGP routing process to compare identical routes received from different external peers during the best path selection process and selects the route with the lowest router ID as the best path. Defaults to disabled.

Any changes in BGP configuration are applied by restarting the current BGP sessions in the VRFs.

The **no** form of this command returns the BGP routing process to the default operation. By default, BGP selects the route that was received first when two routes with identical attributes are received.

Examples

```
switch(config-bgp)# bgp bestpath compare-routerid  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp bestpath compare-routerid  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp bestpath med confed

bgp bestpath med confed
no bgp bestpath med confed

Description

Compares the identical routes received from the different confederation peers and selects the route with the lowest Multi Exit Discriminator (MED) value as the best path. This behavior is disabled by default.

The **no** form of this command prevents the routing process from considering the MED value.



The selection of other attributes like `as-multi-path relax` and `as-path ignore` will not affect the behavior of this command within a confederation.

Examples

Selecting the route with lowest MED value:

```
switch(config-bgp)# bgp bestpath med confed  
All active BGP sessions in the VRF %s will be restarted.  
Do you want to continue (y/n)?
```

Preventing the routing process from selecting the MED value:

```
switch(config-bgp)# no bgp bestpath med confed  
All active BGP sessions in the VRF %s will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp bestpath bgp-std-selection

```
bgp bestpath bgp-std-selection
no bgp bestpath bgp-std-selection
```

Description

Configures the standard Border Gateway Protocol (BGP) best-path selection process used by major vendors. This command is applied in router configuration mode and is VRF-specific. When enabled, it modifies how redistributed routes are considered during BGP best-path selection.

The **no** form of this command restores the default behavior—HPE-ANW-specific best-path selection. This resets all active BGP peers and may change routing path selection across the network for all BGP peers within the VRF where the command is configured.

Examples

Configuring BGP best-path selection:

```
switch(config-bgp)# bgp bestpath bgp-std-selection
All active BGP sessions in the VRF %s will be restarted and also may change
the routing path selection in the network for all BGP peers in the VRF.
Do you want to continue (y/n)?
```

Restoring to default behavior:

```
switch(config-bgp)# no bgp bestpath bgp-std-selection
All active BGP sessions in the VRF %s will be restarted and also may change
the routing path selection in the network for all BGP peers in the VRF.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

bgp bestpath med missing-as-worst

```
bgp bestpath med missing-as-worst
no bgp bestpath med missing-as-worst
```

Description

Configures a BGP routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute. The path without a MED value is the least desirable path. Any changes in BGP configuration are applied by restarting the current BGP sessions in the VRFs.

The **no** form of this command restores default behavior. The default behavior assigns a value of 0 to the missing MED.

Examples

```
switch(config-bgp)# bgp bestpath med missing-as-worst
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp bestpath med missing-as-worst
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp cluster id

```
bgp cluster-id {<IPv4-ADDR> | <ID>}
no bgp cluster-id {<IPv4-ADDR> | <ID>}
```

Description

Specifies the cluster ID when the BGP router is used as a route-reflector. The cluster ID default is the router ID. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command sets the cluster ID to the default value, which is the router ID.

Parameter	Description
<code><IPv4-ADDR></code>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100 .
<code><ID></code>	Specifies the cluster ID as 32-bit number. Range: 1 to 4294967295.

Examples

```
switch(config-bgp)# bgp cluster-id 2.2.2.2
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp cluster-id 2.2.2.2
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp confederation

```
bgp confederation <AS-NUMBER>
no bgp confederation<AS-NUMBER>
```

Description

Configures a BGP confederation with the confederation identifier. The group of Autonomous Systems (ASs) will be presented as a single autonomous system with the confederation identifier as the AS number.

The **no** form of the command deletes the BGP confederation identifier.

Parameter	Description
<AS-NUMBER>	Sets the identifier for the confederation. Range:1-4294967295.

Examples

Configuring the BGP confederation with the AS number:

```
switch(config-bgp)# bgp confederation 100
```

Deleting BGP confederation identifier:

```
switch(config-bgp)# no bgp confederation 100
This will delete BGP confederation identifier on this device.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp confederation peers

```
bgp confederation peers <AS NUMBER>
no bgp bgp confederation peers <AS NUMBER>
```

Description

Configures BGP confederation peers with both same and different sub-autonomous system to establish an eBGP membership. You can configure a list of AS numbers separated by spaces.

The **no** form of this command disables the peer session and deletes the peer information.

Parameter	Description
<AS NUMBER>	Specifies the autonomous system numbers to establish an eBGP membership. Range: 64512-65535.

Examples

```
switch(config-bgp)# bgp confederation peers 64512 64513
```

```
switch(config-bgp)# no bgp confederation peers 64512
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp dampening

```
bgp dampening {{half-life <HALF-TIME> reuse <LOW-THRESHOLD> suppress <HI-THRESHOLD> max-  
suppress-time <MAX-TIME>}  
| route-map <NAME>}
```

Description

Enables route flap dampening which reduces the propagation of unstable routes in the network.

Parameter	Description
half-life <HALF-TIME>	Specifies the half-life time in minutes. When the time expires, the penalty on a route gets reduced exponentially to half its current value. Default: 15.
reuse <LOW-THRESHOLD>	Specifies the lower threshold of penalty. On a suppressed route, when the penalty on a route falls below this value, the route is unsuppressed. Default: 750.
suppress <HI-THRESHOLD>	Specifies the upper threshold of penalty. When the penalty on a flapping route exceeds this value, the route is suppressed. Default: 2000.
max-suppress-time <MAX-TIME>	Specifies the maximum time to keep a route suppressed in minutes. Once this timer expires, the route is unsuppressed. Default: 60.
route-map <NAME>	Specifies the name of a route map.

These parameters can be configured at the router level for specific address families or the same parameters can be configured under a route map which can be applied to dampening command.

Usage

The dampening algorithm assigns a penalty of 1000 to a flapping route every time the route gets withdrawn. The penalty values accumulate on the route every time it flaps. However, the penalty decays and is reduced to half its value by the half-life time.



This feature is not applicable on IBGP routes.

Example

```
switch(config)# router bgp 1
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# bgp dampening

switch(config-bgp-ipv4-uc)# bgp dampening route-map abc

switch(config-bgp-ipv4-uc)# bgp dampening route-map xyz

switch(config-bgp-ipv4-uc)# bgp dampening half-life 10 reuse 100 suppress 250 max-
suppress-time 45
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc	Administrators or local user group members with execution rights for this command.

bgp default local-preference

```
bgp default local-preference <NUMBER>
no bgp default local-preference
```

Description

Default local preference value for BGP learned routes. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command sets the local preference to the default value of 100.

Parameter	Description
<NUMBER>	Specifies the local preference value. Range: 0 to 4294967295. Default: 100.

Examples

```
switch(config-bgp)# bgp default local-preference 20  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp default local-preference  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp deterministic-med

```
bgp deterministic-med  
no bgp deterministic-med
```

Description

Enables comparison of the Multi-Exit Discriminator (MED) attribute when selecting routes advertised by different peers in the same autonomous system. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command sets MED comparison to the default setting of disabled.

Examples

```
switch(config-bgp)# bgp deterministic-med  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp deterministic-med  
All current BGP sessions in VRF default will be restarted.  
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp fast-external-fallover

```
bgp fast-external-fallover  
no bgp fast-external-fallover
```

Description

Sets the switch to reset the BGP sessions of any directly adjacent external peers when the connected link goes down. It is enabled by default.

The **no** form of this command restores the default behavior where BGP waits until the hold time expires before closing sessions.

Examples

```
switch(config-bgp)# bgp fast-external-fallover  
switch(config-bgp)# no bgp fast-external-fallover
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.08	The default behavior has been changed from disabled to enabled state. NOTE: When upgrading, the feature will remain in the state it was (disabled or enabled) in the earlier release.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp graceful-restart restart-time

```
bgp graceful-restart restart-time <DELAY>
no bgp graceful-restart restart-time
```

Description

Sets the graceful restart timer which determines how long the switch waits for a graceful-restart capable neighbor to re-establish BGP peering. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command resets to the default value of 120 seconds.

Parameter	Description
<DELAY>	Graceful restart timer delay in seconds. Range: 1 to 3600. Default: 1500.

Usage

- Graceful restart functionality is enabled by default, and there is no command to disable the functionality at the protocol level.
- However, the graceful-restart functionality can be disabled globally using the command **router graceful-restart**.

Examples

```
switch(config-bgp)# bgp graceful-restart restart-time 150
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp graceful-restart restart-time
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp graceful-restart stalepath-time

```
bgp graceful-restart stalepath-time <TIME>
no bgp graceful-restart stalepath-time
```

Description

Sets the stale path timer. This timer determines how long BGP keeps stale routes from the restarting BGP peer. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command resets to the stale path timer to the default of 300 seconds.

Parameter	Description
<TIME>	Specifies the stale path timer in seconds. Range: 1 to 3600. Default: 300.

Examples

```
switch(config-bgp)# bgp graceful-restart stalepath-time 300
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp graceful-restart stalepath-time
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp log-neighbor-changes

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

Description

Enables logging of BGP neighbor session state changes.

The **no** form of this command disables logging of changes in BGP neighbor adjacencies.

Examples

```
switch(config-bgp) # bgp log-neighbor-changes  
switch(config-bgp) # no bgp log-neighbor-changes
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp maxas-limit

```
bgp maxas-limit <LENGTH>  
no bgp maxas-limit
```

Description

Specifies the maximum size of AS paths in update messages. Routes with AS paths greater than the specified length are discarded.

The **no** form of this command sets the limit to the default of 32.

Parameter	Description
<LENGTH>	Specifies the number of AS segments. Length: 1 to 32 characters. Default: 32.

Example

```
switch(config-bgp) # bgp maxas-limit 20  
switch(config-bgp) # no bgp maxas-limit
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp router-id

```
bgp router-id <ROUTER-ID>
no bgp router-id <ROUTER-ID>
```

Description

Configures a fixed router ID for the BGP peer process running on the router. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

The **no** form of this command removes the fixed router ID from the running configuration and restores the default router ID selection.

Parameter	Description
<ROUTER-ID>	Specifies the router ID in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. If router-id is changed, then all the active BGP peer sessions go down and restart with the newly configured router-id.

Usage

BGP determines the router ID as follows:

1. The address configured with the command `bgp router-id`.
2. The highest IP address on all the loopback interfaces.
3. The highest IP address on any interface.

Examples

```
switch(config-bgp)# bgp router-id 1.1.1.1
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```

```
switch(config-bgp)# no bgp router-id 1.1.1.1
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

bgp update-group

bgp update-group
no bgp update-group

Description

Enables the update-group feature. Update-group is used to optimize BGP processing. With update-group enabled, neighbors that share same outbound policy are grouped under single update-group and update messages are shared to all peers within that group. Disabled by default.

On enabling/disabling update-group, all the current BGP sessions including dynamic peer sessions will be restarted. The dynamic peer sessions will get re-established based on the connect-retry timer configured on the peer device.

BGP determines the AS number size to be used with each individual peer based on the configured AS octet-size on the peers. If BGP is configured to use 2 octet ASN with peer A and 4 octet ASN with peer B, then BGP updates sends to peer A and peer B will be different. Therefore, they will form into two different update-groups.

This feature is supported for IBGP alone. It is not recommended to enable update-group on VPNv4 address families or configure update-group if an VPNv4 address family is configured. Update-group indices are created automatically and cannot be configured. Indices are ephemeral in nature. Update-group indices will not be retained across process restart. When update-group is configured, route reflector clients and non route reflector clients are parted into different update-groups. The use of update-groups imposes the following limitations in BGP processing:

1. While advertising routes to peers of the update-group, the check on route's next-hop is ignored. This means that, BGP routes can get advertised to a peer even if the next-hop IP of the routes is same as peer's IP, and the peer should discard such routes.
2. The use of ORF is restricted. BGP will continue to send outbound route filters to peers, but received filters are ignored.
3. Sender loop detection is delayed until the point where UPDATE messages are sent to the members of the update-group. This means route dropped by the sender due to loop detection will still count as advertised, as they have been advertised to the update-groups.

It is recommended to enable BGP update-group globally before configuring BGP neighbors. This ensures that toggling of BGP neighborhood can be avoided and memory of the routing process can be optimized.

The **no** form of this command disables the update-group feature.

Examples

Enabling BGP update-group:

```
switch(config-bgp)# bgp update-group
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```

Disabling BGP update-group:


```
switch(config-bgp)# no bgp update-group
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

clear bgp

```
clear bgp [vrf <VRF-NAME>][ip unicast | ipv6 unicast | l2vpn evpn | all]
{* | <NEIGHBOR-IP-ADDRESS> | <PEER-GROUP-NAME> } [soft {in | out} ]
```

Description

Clears BGP with a hard or soft reset. If the address-family is specified, then the neighbors that negotiated the respective family will be reset or a route refresh message will be sent.

A route refresh message is sent when **soft in** or **soft out** is specified.

Parameter	Description
ip unicast	Specifies the IPv4 address family.
ipv6 unicast	Specifies the IPv6 address family.
l2vpn evpn	Selects the L2VPN EVPN address family
vrf <VRF-NAME>	Specifies a VRF name. By default, the default BGP instance information is displayed if the VRF is not specified.
all	Specifies all VRFs and address families.
* <NEIGHBOR-IP-ADDRESS> <PEER-GROUP-NAME>	Specifies a neighbor IP address or peer group name for which peer sessions are to be reset, or * to reset all sessions.
soft in	Clears the BGP in the inbound direction without a hard reset of the session. This will send a route refresh request message.

Parameter	Description
soft out	Clears the BGP in the outbound direction without a hard reset of the session. This will send a route refresh message.

Examples

```
switch(config)# clear bgp all *
```

```
switch# clear bgp all PEER_GRP_1 soft in
switch# clear bgp all PEER_GRP_1 soft out
```

```
switch# clear bgp ip unicast 9.0.0.2 soft in
switch# clear bgp ip unicast 9.0.0.2 soft out
switch# clear bgp ip unicast PEER_GRP_1 soft in
switch# clear bgp ip unicast PEER_GRP_1 soft out
```

```
switch# clear bgp vrf v1 ip unicast 9.0.0.2 soft in
switch# clear bgp vrf v1 ip unicast 9.0.0.2 soft out
switch# clear bgp vrf v1 ip unicast PEER_GRP_1 soft in
switch# clear bgp vrf v1 ip unicast PEER_GRP_1 soft out
switch# clear bgp vrf v1 all PEER_GRP_1 soft in
switch# clear bgp vrf v1 all PEER_GRP_1 soft out
```

```
switch# clear bgp ipv6 unicast 9000::2 soft in
switch# clear bgp ipv6 unicast 9000::2 soft out
switch# clear bgp vrf v1 ipv6 unicast 9000::2 soft in
switch# clear bgp vrf v1 ipv6 unicast 9000::2 soft out
```

```
switch# clear bgp l2vpn evpn * soft in
switch# clear bgp l2vpn evpn * soft out
switch# clear bgp l2vpn evpn 9.0.0.2 soft in
switch# clear bgp l2vpn evpn 9.0.0.2 soft out
switch# clear bgp l2vpn evpn PEER_GRP_1 soft in
switch# clear bgp l2vpn evpn PEER_GRP_1 soft out
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	soft out and <PEER-GROUP-NAME> soft in parameters are added.
10.14	Replaced IPv4 with IP in commands. IPv4 is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

disable | enable

disable | enable

Description

This command disables or enables the BGP instance while retaining the configuration. Disable and enable of the BGP instance may result in a change of the router ID.

By default the BGP instance is enabled.

Examples

```
switch(config)# router bgp 100  
switch(config-bgp)# disable
```



The routes learned from a peer will not be removed immediately from the BGP's local RIB when the BGP session on the peer device is disabled. The peer routes experience a graceful restart.



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

distance bgp

```
distance bgp <EXTERNAL> <INTERNAL>  
no distance bgp <EXTERNAL> <INTERNAL>
```

Description

Configures the administrative distance for BGP.

The **no** form of this command restores the default settings, 20 for eBGP and 200 for iBGP,

Parameter	Description
<EXTERNAL>	Specifies the administrative distance for eBGP routes. Range: 1 to 255. Default: 20.
<INTERNAL>	Specifies the administrative distance for iBGP routes. Range: 1 to 255. Default: 200.

Example

```
switch(config-bgp-ipv4-uc) # distance bgp 100 150
switch(config-bgp-ipv4-uc) # no distance bgp 100 150
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

maximum-paths

```
maximum-paths <MAXPATHS>
no maximum-paths <MAXPATHS>
```

Description

Configures the maximum number of paths that BGP adds to the route table for equal-cost multipath (ECMP) load balancing for routes learned from both internal and external BGP. Any changes in BGP configuration are applied by restarting the current BGP sessions on the VRFs.

On HPE Aruba Networking 8325, 8325H, 8325P and 10000 switch series, a maximum-paths configuration is supported globally as well as for **ipv4-unicast**, **ipv6-unicast** and **l2vpn-evpn** address families. For HPE Aruba Networking 8325, 8325H, and 10000 switch series, this configuration is supported under the **l2vpn-evpn** for L2/L3 Overlay ECMP feature. On HPE Aruba Networking 6300, 6400, 8100 and 8360 switch series, this command is supported under the **l2vpn-evpn** for L2 Overlay ECMP feature.

If address-family specific maximum-paths are configured, they take precedence over global configuration. Greater than eight maximum-paths at can be configured within the global context, but for **l2vpn-evpn** routes the supported maximum limit is still eight.

The **no** form of this command restores the default setting of 4.

Parameter	Description
<MAXPATHS>	Specifies the maximum number of paths. 1 to 32 paths can be set globally. 1 to 8 paths can be set for l2vpn-evpn address family. 1 to 32 paths can be set for ipv4-unicast and ipv6-unicast .

Usage

When both global and address-family maximum paths are configured then the address family value takes precedence.

Global max-path	l2evpn, ipv4-unicast, or ipv6-unicast address-family Max-path	Operational Max-path	Comments
Default(4)	Default (4)	4	--
Configured (4)	configured (4)	4	Four is the configured value for address family paths
Default (4)	8 (max)	8	The address family value takes precedence
32 (max)	8 (max)	8	CLI configuration is limited to eight paths.
Default (8)	configured (4)	4	Four is the configured value for address family paths

Examples

Configuring the maximum number of global paths:

```
switch(config)# router bgp 1
switch(config-bgp)# maximum-paths 32
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)? y
```

Configuring the maximum-paths for the l2vpn-evpn address family:

```
switch(config-bgp)# address-family l2vpn evpn
switch(config-bgp-l2vpn-evpn)# maximum-paths 6
```

Removing the global maximum paths setting:

```
switch(config-bgp)# no maximum-paths
All current BGP sessions in VRF default will be restarted.
Do you want to continue (y/n)? y
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.13.1000	On 8325, 8325H, 8325P and 10000 switch series, configuration is supported on ipv4-unicast , ipv6-unicast and l2vpn-evpn address families. For HPE Aruba Networking 6300, 6400, 8100, 8360, 8400 and 9300 Switch series, this configuration is supported at the global level only.
10.10	Increased upper limit of range of <i><MAXPATHS></i> parameter to 32.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-bgp	Administrators or local user group members with execution rights for this command.
9300S	config-bgp-l2vpn-evpn	

neighbor activate

```
neighbor {<IP-ADDR>|<IFNAME>} activate
no neighbor {<IP-ADDR>|<IFNAME>} activate
```

Description

This command enables the address-family capability and exchange of information specific to an address family with a BGP neighbor.

The **no** form of this command removes the address-family capability and disables the exchange of routes for the specified address-family with the BGP neighbor.

Parameter	Description
<i><IP-ADDR></i>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Specifies the unnumbered interface name of the neighbor.
<i><IFNAME></i>	Specifies the unnumbered interface name of the neighbor.



VPNv4 address-family, peer group, and BFD are not supported for BGP unnumbered.

Examples

Enabling and removing the address-family capability and exchange of information on 1/1/1.

```
switch(config-bgp) # neighbor 1/1/1 remote-as 1
switch(config-bgp-ipv4-uc) # neighbor 1/1/1 activate
switch(config-bgp-ipv4-uc) # no neighbor 1/1/1 activate
```

Enabling and removing the address-family capability and exchange of information on 1/1/1.1.

```
switch(config-bgp)# neighbor 1/1/1.1
switch(config-bgp-ipv6-uc)# neighbor 1/1/1.1 activate
switch(config-bgp-ipv6-uc)# no neighbor 1/1/1.1 activate
```

Enabling and removing the address-family capability and exchange of information on 1/1/1:1.

```
switch(config-bgp)# neighbor 1/1/1:1
switch(config-bgp-ipv4-uc)# neighbor 1/1/1:1 activate
switch(config-bgp-ipv4-uc)# no neighbor 1/1/1:1 activate
```

Enabling and removing the address-family capability and exchange of information on 1.1.1.1.

```
switch(config-bgp-l2vpn-evpn)# neighbor 1.1.1.1 activate
switch(config-bgp-l2vpn-evpn)# no neighbor 1.1.1.1 activate
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor advertisement-interval

```
neighbor {<IP-ADDRESS>|<IFNAME>|<PEER-GROUP-NAME>} advertisement-interval <INTERVAL>
no neighbor {<IP-ADDRESS>|<IFNAME>|<PEER-GROUP-NAME>} advertisement-interval
```

Description

Sets the advertisement interval, which defines the length of time between transmission of BGP routing updates.

The **no** form of this command restores the default value. Default values are 30 seconds for external BGP peer and 5 seconds for internal BGP peer.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format

Parameter	Description
	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a Peer-Group. This is not supported on BGP unnumbered.
<INTERVAL>	Specifies the advertisement interval in seconds. Range: 0 to 600. Default: 30 for external BGP peer and 5 for internal BGP peer.

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 advertisement-interval 20
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 advertisement-interval
```

```
switch(config-bgp-ipv4-uc) # neighbor pg advertisement-interval 50
switch(config-bgp-ipv4-uc) # no neighbor pg advertisement-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor add-paths

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} add-paths {send | recv | both}
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} add-paths {send | recv | both}
```

Description

Enables additional path capability for BGP as described in RFC 7911. This allows BGP peer to send, receive, or send and receive multiple paths for the same address prefix without the subsequent advertisements implicitly replacing any previous paths. The additional path includes the first (N-1) best paths, which means that the total paths for an address prefix received by a BGP speaker will include the best path and the additional paths determined by its BGP peer.

With additional path feature, each path is identified by a path identifier in addition to the address prefix. To use this command, the backup path of BGP next-hop must be different than the primary path.

The **no** form of this command disables the additional path feature.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
add-paths {send recv both}	Configures the additional paths in one of the following ways: send—Enables the neighbor to send the additional paths. recv—Enables the neighbor to receive the additional paths. both—Enables the neighbor to send and receive the additional paths.

Examples

Enabling BGP neighbor to send the additional paths:

```
switch(config)# router bgp 100
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# neighbor 1.1.1.1 add-paths send
```

Disabling BGP neighbor to send the additional paths:

```
switch(config)# router bgp 100
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# no neighbor 1.1.1.1 add-paths send
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor add-paths advertise-best

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} add-paths advertise-best <2-4>
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} add-paths advertise-best <2-4>
```

Description

Controls the number of best BGP Paths to be advertised by a BGP speaker to a BGP peer. When enabled, it allows BGP speaker to advertise more than one best paths for the same address prefix. The total paths for an address prefix will include the best path and the additional paths.

The **no** form of this command removes the advertise best path configuration.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
advertise-best <2-4>	Specifies the number of best BGP paths to be advertised to a BGP Peer. Range: 2 to 4. Default: 2.

Examples

Setting the number of best paths to send to the neighbor:

```
switch(config)# router bgp 100
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# neighbor 1.1.1.1 add-paths advertise-best 3
```

Removing the advertise best path configuration:

```
switch(config)# router bgp 100
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# no neighbor 1.1.1.1 add-paths advertise-best 3
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor allowas-in

```
neighbor {<IP-ADDRESS>|<IFNAME>|<LIMIT>}
no neighbor {<IP-ADDRESS>|<IFNAME>|<LIMIT>}
```

Description

Specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP speaker and still be accepted. When this configuration is applied to a peer-group, all the neighbors that are part of the peer-group inherit this setting.

The **no** form of this command restores the default setting, which is to reject as a loop any route where the path contains the speaker AS number.

Parameter	Description
<code><IP-ADDRESS></code>	Specifies the neighbor IP address in the IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or in the IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. NOTE: IPv6 MP-BGP peering must not be used for L2VPN EVPN address family, because VXLAN tunnel interface does not support IPv6 addresses.
<code><IFNAME></code>	Specifies the unnumbered interface name of the neighbor.
<code><PEER-GROUP-NAME></code>	Specifies a peer group.
<code><LIMIT></code>	Specifies the number of times that the AS path of a received route can contain the AS number of the recipient BGP. Range: 1 to 10.

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 allowas-in 5
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 allowas-in
```

```
switch(config-bgp-ipv6-uc) # neighbor 2001:0db8:85a3::8a2e:0370:7334 allowas-in 5
switch(config-bgp-ipv6-uc) # no neighbor 2001:0db8:85a3::8a2e:0370:7334 allowas-in
```

```
switch(config-bgp-ipv4-uc) # neighbor PG allowas-in 5
switch(config-bgp-ipv4-uc) # no neighbor PG allowas-in
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 1.1.1.1 allowas-in 5
switch(config-bgp-l2vpn-evpn) # no neighbor 1.1.1.1 allowas-in
```

```
switch(config-bgp-l2vpn-evpn) # neighbor PG allowas-in 5
switch(config-bgp-l2vpn-evpn) # no neighbor PG allowas-in
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 2001:0db8:85a3::8a2e:0370:7334 allowas-in 5
switch(config-bgp-l2vpn-evpn) # no neighbor 2001:0db8:85a3::8a2e:0370:7334 allowas-in
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor ao

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} ao <keychain-name>
  accept-ao-mismatch
  include-tcp-options
  no ...
```

Description

Enables TCP Authentication Option (TCP-AO) authentication on a TCP connection between two BGP neighbors. To disable this function, use the **no** form of this command.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<keychain-name>	Name of the keychain for the neighbor. The keychain allows keys to be configured with different valid lifetimes. This mechanism provides a way for a set of keys to be rotated and hence protect against long-lived-key attacks. At any given time only one key is selected as active-key and keys are valid for a duration of the defined send-lifetime. If the send-lifetime and the accept-lifetimes are not configured for the key, the key is considered to be valid for infinite lifetime.

Parameter	Description
	When multiple keys are configured, its recommended that keys overlap in their send-lifetimes so that the key rollover occurs at the start of the next key's send-lifetime. This allows for a continuous key usage by TCP-AO.
<code>accept-ao-mismatch</code>	Accept incoming TCP segments without TCP-AO option. If enabled, the device will accept a connection from the peer <i>even if the received TCP packets do not contain the TCP-AO option</i> .
<code>include-tcp-options</code>	Include the TCP header options for MAC calculation. Note that enabling this setting will immediately reset the neighbor session. This setting is disabled by default.
<code>no ...</code>	Negates any configured parameter.

Usage

TCP-AO authentication can not be used with the [neighbor password](#) feature. When TCP-AO is applied to a peer-group, all the neighbors in peer-group will inherit the peer-group configuration unless there is a configuration specific to an individual neighbor. If a peer-group is configured with the neighbor password feature but the neighbors that belong to that peer-group are configured with TCP-AO, the TCP-AO configuration will be rejected. Similarly, If a peer-group is configured to use TCP-AO authentication, the neighbors that belong to that peer-group will reject the neighbor password.

The TCP-AO feature takes a keychain as a parameter. The key will not be valid until a [Recv-D](#), [Send-ID](#), and [send lifetime](#) is configured. The supported cryptographic algorithms for TCP-AO are:

- HMAC-SHA-1-96 based on [RFC2104] and [FIPS-180-3]
- AES-128-CMAC-96 based on [NIST-SP800-38B][FIPS197]

Examples

```
switch(config)# keychain bgpkeys
switch(config-keychain)# key 1
switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2022 duration
infinite
switch(config-keychain-key)# accept-lifetime start-time 10:10:10 10/25/2022
duration infinite
switch(config-keychain-key)# send-id 10
switch(config-keychain-key)# recv-id 10
switch(config-keychain-key)# cryptographic-algorithm aes-cmac-128
switch(config-keychain-key)# key-string plaintext qwer
switch(config)# router bgp 1
switch(config-bgp)# neighbor 1.1.1.1 ao bgpkeys
switch(config-bgp)# no neighbor 1.1.1.1 ao accept-ao-mismatch
switch(config-bgp)# no neighbor 1.1.1.1 ao include-tcp-option
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.11 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor capability orf prefix-list

```
neighbor {<IP-ADDRESS>|<IFNAME>} capability orf prefix-list {send | receive | both}
no neighbor {<IP-ADDRESS>|<IFNAME>} capability orf prefix-list {send | receive | both}
```

Description

Enables the Outbound Route filtering (ORF) capability with the neighbor in one of the three available modes. The available modes are send, receive, and both. The ORF capability is executed based on prefix list only.

The Outbound Route Filtering (ORF) capability provides a mechanism for a BGP speaker to send a set of Outbound Route Filters (ORFs) that can be used by its BGP peer to filter its outbound routing updates to the speaker. This is a filtering method used to reduce the computation on the router receiving the route.

The **no** form of this command disables the ORF capability.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
capability orf prefix-list {send receive both}	Enables ORF prefix list capability with the neighbor in one of the following modes: ▪ send - Enables the ORF prefix list capability in send mode. ▪ receive - Enables the ORF prefix list capability in receive mode. ▪ both - Enables the ORF prefix list capability in both send and receive mode.

Examples

Enabling the ORF prefix list capability in both send and receive mode:

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 capability orf prefix-list both
```

Enabling the ORF prefix list capability in send mode:

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 capability orf prefix-list send
```

Disabling the ORF prefix list capability in both send and receive mode: :

```
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 capability orf prefix-list both
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor default-originate

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} default-originate [route-map <MAP-NAME>]  
no neighbor {<IP-ADDRESS>|<IFNAME>|<PEER-GROUP-NAME>} default-originate [route-map <MAP-NAME>]
```

Description

Enables the local router to send the default route 0.0.0.0 to a neighbor. The neighbor can then use this route to reach the router when all other routes are unavailable. Use the `route-map` option to configure the route map to modify the default route attributes.

The **no** form of this command disables this feature.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<MAP-NAME>	Sets the route map to modify the default route attributes.

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 default-originate
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 default-originate
```

```
switch(config-bgp-ipv4-uc) # neighbor PG default-originate
switch(config-bgp-ipv4-uc) # no neighbor PG default-originate
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor ebgp-multihop

```
neighbor {<IP-ADDR> | <PEER-GROUP-NAME>} ebgp-multihop <ttl>
no neighbor {<IP-ADDR> | <PEER-GROUP-NAME>} ebgp-multihop <ttl>
```

Description

Enables BGP to establish a session with external peers residing on networks that are not directly connected. By default, BGP can only establish sessions with external BGP peers that are directly connected. If external BGP peer are not connected directly, then ebgp-multihop is enabled to initiate the connection with that external peer. If ebgp-multihop is disabled and external BGP peers are indirectly connected, then BGP peer session is not established.

The **no** form of this command disables the peer ebgp-multihop feature.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<PEER-GROUP-NAME>	Specifies a peer group.
<ttl>	Specifies the ttl value.

Examples

Enabling BGP to establish connection with external peers residing on networks that are not directly connected:


```
switch(config-bgp) # neighbor 1.1.1.1 ebgp-multihop 5
```

Disabling BGP to establish connection with external peers residing on networks that are not directly connected:

```
switch(config-bgp) # no neighbor 1.1.1.1 ebgp-multihop
```

Enabling BGP to establish connection with external peers residing on networks that are not directly connected:

```
switch(config-bgp) # neighbor pg ebgp-multihop 5
```

Disabling BGP to establish connection with external peers residing on networks that are not directly connected:

```
switch(config-bgp) # no neighbor pg ebgp-multihop 5
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Syntax updated to use <ttl> instead of <HOP-COUNT>.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor fall-over

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} fall-over  
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} fall-over
```

Description

Enables BGP fast peering session deactivation. When neighbor fall-over is configured, the BGP process monitors the RIB and if the route to peer is not present in the routing table, it immediately deactivates the peer session without waiting for the hold down timer. It is disabled by default.

The **no** form of this command disables this feature.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.

Usage

Neighbor fall-over does not track connected or static routes to peers. However, this is not an issue when IBGP peering is using a loopback interface. To force a fall-over for connected and static routes, use the command `neighbor fall-over bfd`.

Examples

```
switch(config-bgp)# neighbor 1.1.1.1 fall-over
switch(config-bgp)# no neighbor 1.1.1.1 fall-over
```

```
switch(config-bgp)# neighbor PG fall-over
switch(config-bgp)# no neighbor PG fall-over
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor fall-over bfd

```
neighbor {<IPV4-ADDR>|<IPV6-ADDR>|<PEER-GROUP-NAME>} fall-over bfd
no neighbor {<IPV4-ADDR>|<IPV6-ADDR>|<PEER-GROUP-NAME>} fall-over bfd
```

Description

Enables BGP to register with BFD to receive fast peering session deactivation messages from BFD. You can either configure BFD support for BGP per neighbor or peer-group.

The **no** form of this command disables BGP for BFD.



Multihop BFD is not supported for BGP.

Parameter	Description
<code><IPv4-ADDR></code>	Specifies the neighbor address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<code><IPv6-ADDR></code>	Specifies the neighbor address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. This parameter applies only to HPE Aruba Networking 6300 and 6400 Switch series.
<code><PEER-GROUP-NAME></code>	Specifies a peer group.

Examples

Enabling BFD for BGP neighbor with IPv4 address:

```
switch(config-bgp)# neighbor 1.1.1.1 fall-over bfd
```

Enabling BFD for BGP neighbor with IPv6 address (applies only to HPE Aruba Networking 6300 and 6400 Switch series):

```
switch(config-bgp)# neighbor 1000::1 fall-over bfd
```

Enabling BFD for peer group:

```
switch(config-bgp)# neighbor PG fall-over bfd
```

Disabling BFD for BGP per neighbor IPv4 address:

```
switch(config-bgp)# no neighbor 1.1.1.1 fall-over bfd
```

Disabling BFD for BGP per neighbor with IPv6 address (applies only to HPE Aruba Networking 6300 and 6400 Switch series):

```
switch(config-bgp)# no neighbor 1000::1 fall-over bfd
```

Disabling BFD for peer group:

```
switch(config-bgp)# no neighbor PG fall-over bfd
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor graceful-shutdown

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} graceful-shutdown
    [local-preference <LOCAL-PREF>
    | <CONFIG-DELAY>
    |<LOCAL-PREF> ]
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} graceful-shutdown
    [local-preference <LOCAL-PREF>
    | <CONFIG-DELAY>
    |<LOCAL-PREF> ]
```

Description

Configures the wait time before shutting down the BGP neighbor session, and can also configure the local preference value to be advertised before graceful shutdown.

The **no** form of this command sets the wait time to the default value of 180 seconds and the local-preference value to the default of 0.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
local-preference<LOCAL-PREF>	Specifies the local preference value for exporting the iBGP routes during a graceful shutdown. The lower the value, the lower the local preference. A value of 0 indicates that the route is the least preferred. Range: 0 to 4294967295. Default: 0.
<CONFIG-DELAY>	Specifies the time to wait before shutting down the neighbor in seconds. Range: 10 to 1200. Default: 180.

Usage

If the graceful shutdown timer has already started and the administrator configures a command that triggers a session restart, traffic loss can occur if the graceful shutdown delay is not sufficient for the BGP peers to converge to a new route.



On each Autonomous System Boundary Router (ASBR) supporting the graceful shutdown receiver procedure, an inbound BGP route policy must be applied on all EBGP sessions of the ASBR.

The policy must match the GSHUT community and lower the precedence of the route by changing the route attributes.

The Graceful-Shutdown feature does not work for reflected routes because the route reflector (RR) does not modify local-preference attribute. The routes, originated by the RR, carry the GSHUT local-preference value. As per the RFC 4456, when an RR reflects a route, it should not modify the following path attributes:

- NEXT-HOP
- AS-PATH
- LOCAL-PREF
- MED

Their modification could potentially result in routing loops. In this situation, apply on the RR an inbound BGP route policy, meeting the following conditions:

- Match the graceful-shutdown community.
- Set the local preference attributes of the paths tagged with the graceful-shutdown community to a lower value than other routes to the same destination.

Examples

Setting the wait time delay:

```
switch(config-bgp) # neighbor 1.1.1.1 graceful-shutdown 10
```

Setting the local-preference value:

```
switch(config-bgp) # neighbor 1.1.1.1 graceful-shutdown local-preference 100
```

Setting the wait time delay and local-preference value:

```
switch(config-bgp) # neighbor 1.1.1.1 graceful-shutdown 10 local-preference 100
```

Setting the wait time delay to the default of 180 seconds:

```
switch(config-bgp) # no neighbor 1.1.1.1 graceful-shutdown 10
```

Setting the local-preference value to default of 0:

```
switch(config-bgp) # no neighbor 1.1.1.1 graceful-shutdown local-preference 100
```

Setting the wait time delay and local-preference value to defaults:

```
switch(config-bgp) # no neighbor 1.1.1.1 graceful-shutdown 10 local-preference 100
```

Complete deletion:

```
switch(config-bgp) # no neighbor 1.1.1.1 graceful-shutdown
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor interface

```
neighbor {<IP-ADDR>|<IFNAME>} interface <ifname>  
[no] neighbor {<IP-ADDR>|<IFNAME>} interface <ifname>
```

Description

Configure a BGP neighbor by specifying the interface name on which the neighbor is connected instead of the neighbor's IP address. When an unnumbered interface is specified to the **neighbor** command, a static route is auto-provisioned for the neighbor with the unnumbered interface as a destination. A static route is also auto-provisioned if the neighbor IP address is learned via LLDP.



If OSPF is enabled on an unnumbered interface then the auto-provisioning is not supported as the route to the BGP peer is expected to be learned via OSPF.

Peer-group is not supported for BGP peering on the IP unnumbered interface.

The **no** form of this command disables this feature.

Parameter	Description
<IP-ADDR>	Specifies an IP address.

Examples

Configuring unnumbered BGP peering on interface 1/1/1:

```
switch(config)# router bgp 100
switch(config-bgp)# neighbor 1.1.1.1 remote-as 100
switch(config-bgp)# neighbor 1.1.1.1 interface 1/1/1
```

Disabling this feature:

```
switch(config)# router bgp 100
switch(config-bgp)# no neighbor 1.1.1.1 interface 1/1/1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor listen ip-range

```
neighbor <PEER-GROUP-NAME> listen ip-range <IP-ADDR>|<MASK> {as-range <AS-RANGE>|limit <LIMIT>}
no neighbor <PEER-GROUP-NAME> listen ip-range <IP-ADDR>|<MASK> {as-range <AS-RANGE>|limit <LIMIT>}
```

Description

Configures BGP dynamic neighbors as ranges of remote addresses with associated peer groups. The **no** form of this command restores default behavior.



- Each range of remote addresses is configured as a remote address prefix.
- Any BGP peer with a remote address that matches the remote address prefix becomes a member of the associated peer group.

Parameter	Description
<PEER-GROUP-NAME>	Specifies peer group. This is not supported on BGP unnumbered.
<IP-ADDR> <MASK>	Specifies subnet range.
<AS-RANGE>	Specifies AS number as a range in integer or dotted format.

Parameter	Description
<code><LIMIT></code>	Specifies maximum number of peers. Range: 1 to 256.

Restrictions

- Dynamic peers are always passive. Outbound connections to dynamic peers are not supported.
- Dynamic BGP peering is only compatible with peer-groups
- Disabling partial AS range is not supported. The exact value that is configured must be used.
 - When disabling AS range, CLI must use the same AS range that was used when first configured. For example, if AS range "1-4" is configured, when disabling, "1-4" must be used ("1,2,3,4" is not supported).



Configuring overlapping peer ranges with different remote address prefix lengths is not recommended. Peer range configuration is recommended when peer ranges do not overlap.

Usage

- All supported address-families are activated on a dynamic peer for negotiation by default.
- If an incoming connection matches multiple peer range entries, the entry with the longest remote address prefix is selected.
- AS ranges are used to match remote AS presented by connecting peers. Remote AS matching with ASes or AS ranges in this list will be accepted.
 - AS range only applies to dynamic peers.
- The limit option is used to set the maximum number of dynamic BGP peers within the peer range. The default is 512 if no limit is set.
 - If the limit is reached, BGP rejects incoming connections from new dynamic BGP peers until BGP session termination causes the number of dynamic BGP peers to fall below the limit.
 - If the limit is reduced below the current number of dynamic BGP peers, BGP will reject incoming connections from new dynamic BGP peers until the number of dynamic BGP peers falls below the new limit. BGP will not terminate existing BGP sessions with dynamic BGP peers in this case. If an existing BGP session gets terminated, that session will not re-establish until the number of BGP sessions falls below the limit.
- After dynamic peer is configured, additional configuration is required on the peer-group as a whole. Individual member groups are incompatible. For example, the neighbor shutdown command can be executed on a peer-group, but not on individual members of the peer-group.
- When a peer is configured as dynamic and is in an established state, a shutdown is required before reconfiguring as static.
- Connect-retry interval is recommended to be configured with a smaller value than the default value on the active peer.
- When a set of valid and invalid AS values are issued (separated by commas), only the valid values are accepted.
- When the AS range parameter is not explicitly configured in dynamic bgp peering, iBGP session comes up, eBGP session does not. If there are no configured remote AS or AS list entries, DC-BGP assumes that any peer is an iBGP peer.

Examples


```
switch(config-bgp)# neighbor pg listen ip-range 192.168.0.0/16
```

```
switch(config-bgp)# no neighbor pg listen ip-range 192.168.0.0/16
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor local-as

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} local-as <AS-NUMBER> [no-prepend[replace-as[dual-as]]]
```

```
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} local-as [no-prepend[replace-as[dual-as]]]
```

Description

Configures an alternate local AS number that can be used to establish a session with a peer, allowing a router to appear to be a member of a second autonomous system (AS), and its real AS.

Local AS allows two autonomous systems to merge without modifying peering arrangements. This command is valid only for external peers.

The **no** form of this command restores the default, which is for a peering session to be established using the primary AS (primary AS is the AS number specified at the time of neighbor creation using the command `neighbor remote-as`).

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
local-as <AS-NUMBER>	Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers.
no-prepend	Optional. When you include this parameter, the switch will not prepend local ASN value to the AS path list for all the routes received from the peer.

Parameter	Description
<code>replace-as</code>	Optional. Replaces the configured router AS with the local AS in the EBGp updates.
<code>dual-as</code>	Optional. Use this option to form the neighborhood with any of the two AS numbers; the configured router ASN or the local ASN.

Examples

Configuring an alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # neighbor 1.1.1.1 local-as 200
```

Removing the alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # no neighbor 1.1.1.1 local-as 200
```

Configuring an alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # neighbor pg local-as 200 no-prepend
```

Removing the alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # no neighbor pg local-as 200 no-prepend
```

Configuring an alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # neighbor pg local-as 200 no-prepend replace-as
```

Removing the alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # no neighbor pg local-as 200 no-prepend replace-as
```

Configuring an alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # neighbor pg local-as 200 no-prepend replace-as dual-as
```

Removing the alternate local AS number that can be used to establish a session with a peer:

```
switch(config-bgp) # no neighbor pg local-as 200 no-prepend replace-as dual-as
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor maximum-prefix

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>}
    maximum-prefix <MAXIMUM> [threshold <THRESHOLD>]
    [restart <INTERVAL>] [warning-only]
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} maximum-prefix<MAXIMUM> [threshold
<THRESHOLD>]
    [restart <INTERVAL>] [warning-only]
```

Description

Sets the maximum number of prefixes that can be received from a neighbor.

The session is re-established only if the number of routes received from the BGP peer does not exceed the configured prefix limit. When the restart timer is configured, sessions are automatically re-established when the timer expires. By default, the device accepts 128,000 prefixes from a BGP neighbor with a threshold value of 75%. A warning message is generated when the number of prefixes per neighbor reaches 75% of default prefix limit. Another warning message is generated when the default prefix limit is reached. A maximum prefix limit applies at the neighbor level. If maximum-prefix limit exceeds any configured limit, the BGP session with that neighbor will be brought down.

The **no** form of this command disables the maximum number of prefixes limit.

Parameter	Description
<IP-ADDR>	Specifies the IP address of the neighbor in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a Peer-Group. This is not supported on BGP unnumbered.
maximum-prefix <MAXIMUM>	Specifies the maximum number of prefixes allowed from the specified neighbor. Range: 1 to 128000. Default: 128000.
threshold <THRESHOLD>	Specifies at what percentage of MAXIMUM a warning message is generated. Range: 1 to 100. Default: 75. For example, if MAXIMUM is set to 1000 and threshold is 70, the router generates a warning message when the number of BGP learned routes from the neighbor exceeds 70 percent of 1000

Parameter	Description
	(700) routes.
<code>restart <INTERVAL></code>	Specifies interval in seconds for restarting the BGP connection when the prefix limit is exceeded. Range: 30 to 65535.
<code>warning-only</code>	Specifies generating and logging a warning message without disconnecting the BGP session when the prefix limit is exceeded.

Examples

Setting the prefix limit to 1000 prefixes:

```
switch(config-bgp-ipv4-uc) # neighbor 10.0.0.1 maximum-prefix 1000
```

Enabling logging of a warning message when more than 1000 prefixes are received:

```
switch(config-bgp-ipv4-uc) # neighbor 10.0.0.1 maximum-prefix 1000 warning-only
```

Setting the prefix limit to 1000 prefixes and enabling logging of a warning message when 500 prefixes are received:

```
switch(config-bgp-ipv4-uc) # neighbor 10.0.0.1 maximum-prefix 1000 threshold 50
```

Setting the prefix limit to 1000 prefixes and enabling logging of a warning message when 500 prefixes are received and a second warning when the prefix limit is exceeded without disconnecting the session:

```
switch(config-bgp-ipv4-uc) # neighbor 10.0.0.1 maximum-prefix 1000 threshold 50
warning-only
```

Removing the threshold value:

```
switch(config-bgp-ipv4-uc) # no neighbor 10.0.0.1 maximum-prefix 1000 threshold 50
```

Disabling the maximum-prefix feature:

```
switch(config-bgp-ipv4-uc) # no neighbor 10.0.0.1 maximum-prefix
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor next-hop-self

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>}next-hop-self  
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} next-hop-self
```

Description

Configures the router as the next hop for a BGP-speaking neighbor or peer group, and enables BGP to send itself as the next hop for advertised routes.

The **no** form of this command resets the peer next-hop-self status to default. The next hop is generated based on the IP.

Parameter	Description
<IP-ADDR>	Specifies the neighbor's IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
all	Applies the configuration to all route-reflector clients.

Usage

- An administrator uses this command to make a BGP speaker fill its address when advertising routes to a BGP peer.
- This command is useful in non-meshed networks where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.
- While advertising routes to eBGP peers, the next-hop is set to self IP by default. The default behavior can be changed by configuring next-hop-unchanged.
- While advertising routes to iBGP peers, the next-hop is kept unchanged by default. The default behavior can be changed by configuring next-hop-self.

BGP L2VPN EVPN context:

- The next-hop-self command under l2vpn-evpn address-family, in addition to replacing the next-hop IP of EVPN routes with self IP, replaces the routers-mac extended community of EVPN routes with self MAC.

Examples

BGP IPv4 UC context:

Setting and resetting the router as the next hop self for neighbor 1.1.1.1:

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 next-hop-self
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 next-hop-self
```

Setting and resetting the router as the next hop self for its peer group:

```
switch(config-bgp-ipv4-uc) # neighbor pg next-hop-self
switch(config-bgp-ipv4-uc) # no neighbor pg next-hop-self
```

BGP L2VPN EVPN context:

Setting and resetting the router as the next hop self for neighbor 1.1.1.1:

```
switch(config-bgp-l2vpn-evpn) # neighbor 1.1.1.1 next-hop-self
switch(config-bgp-l2vpn-evpn) # no neighbor 1.1.1.1 next-hop-self
```

Setting and resetting the router as the next hop self for its peer group:

```
switch(config-bgp-l2vpn-evpn) # neighbor pg next-hop-self
switch(config-bgp-l2vpn-evpn) # no neighbor pg next-hop-self
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.9	Added support for BGP L2VPN EVPN address family.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor next-hop-unchanged

```
neighbor {<IP-ADDRESS>|<IFNAME>} next-hop-unchanged
no neighbor {<IP-ADDRESS>|<IFNAME>} next-hop-unchanged
```

Description

Enables the neighbor to preserve next-hop while advertising routes to eBGP peers, in the L2VPN EVPN address-family.

The **no** form of this command resets the peer next-hop-unchanged status to default.

Parameter	Description
<code><IP-ADDRESS></code>	Specifies the neighbor IP address in the IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or in the IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. NOTE: IPv6 MP-BGP peering must not be used for L2VPN EVPN address family, because VXLAN tunnel interface does not support IPv6 addresses.
<code><IFNAME></code>	Specifies the unnumbered interface name of the neighbor.

Examples

```
switch(config-bgp-l2vpn-evpn)# neighbor 1.1.1.1 next-hop-unchanged
```

```
switch(config-bgp-l2vpn-evpn)# neighbor 2001:0db8:85a3::8a2e:0370:7334 next-hop-unchanged
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor orf prefix-list in

```
neighbor {<IP-ADDRESS>|<IFNAME>} orf-prefix-list <PREFIX-LIST-NAME> in
no neighbor {<IP-ADDRESS>|<IFNAME>} orf-prefix-list <PREFIX-LIST-NAME> in
```

Description

Applies an inbound prefix list filter to filter the distribution of BGP neighbor information. The **no** form of this command restores the default behavior of not applying the prefix list filter.



This command must be used only along with the ORF capability to take effect.

Parameter	Description
<code><IP-ADDRESS></code>	Specifies an IP address.
<code><IFNAME></code>	Specifies the unnumbered interface name of the neighbor.
<code>orf-prefix-list PREFIX-LIST-NAME></code>	Sends the prefix list name to be filtered.

Usage

To use this command, the following conditions must be met:

- If route-map inbound is also applied on multiple neighbors along with ORF, then the route-map name must be common on all the neighbors.
- If route-map inbound is also applied on an IPv6 AF BGP neighbor, then the route-map sequence number with value 1 cannot be used.

Examples

Applying the inbound prefix list filter:

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 orf-prefix-list ABC in
```

Removing the inbound prefix list filter:

```
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 orf-prefix-list ABC in
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

neighbor passive

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} passive
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} passive
```

Description

Configures a specific neighbor, or all neighbors in a peer-group, as passive, which means that they will not initiate the TCP session.

The **no** form of this command enables the neighbor to initiate the TCP session.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group.

Examples

Configure a specific neighbor as passive:

```
switch(config-bgp) # neighbor 1.1.1.1 passive
```

Enabling the local router to initiate the TCP session for a specified neighbor:

```
switch(config-bgp) # no neighbor 1.1.1.1 passive
```

Configure a specific peer group as passive:

```
switch(config-bgp) # neighbor pg passive
```

Enabling the local router to initiate the TCP session for a specified peer group:

```
switch(config-bgp) # no neighbor pg passive
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor password

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} password [{ciphertext | plaintext}
<PASSWORD>]
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>}
password [ciphertext <PASSWORD>]
```

Description

Enables message digest5 (MD5) authentication on a TCP connection between two BGP neighbors. When the password is applied to a peer-group, all the neighbors that are part of peer-group inherit the configured setting.

The **no** form of this command removes the neighbor password.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a Peer-Group. This is not supported on BGP unnumbered.
{ciphertext plaintext}	Selects the password format.
<PASSWORD>	Specifies the password.



When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Enabling message digest5 (MD5) authentication for a neighbor with a provided plaintext password:

```
switch(config-bgp)# neighbor 1.1.1.1 password plaintext doubt_Plane#93
```

Enabling message digest5 (MD5) authentication for a neighbor with a prompted plaintext password:

```
switch(config-bgp)# neighbor 1.1.1.5 password
Enter the neighbor password: *****
Re-Enter the neighbor password: *****
```

Enabling message digest5 (MD5) authentication for a peer group with a provided plaintext password:

```
switch(config-bgp)# neighbor pg_3 password plaintext doubt_Plane#93
```

Disabling message digest5 (MD5) authentication for a neighbor:

```
switch(config-bgp)# no neighbor 1.1.1.5 password
```

Disabling message digest5 (MD5) authentication for a peer group:

```
switch(config-bgp) # no neighbor pg_3 password
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor port

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} port <NUMBER>  
no neighbor{<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} port <NUMBER>
```

Description

Sets a custom TCP port on which to communicate with the BGP neighbor.

When this configuration is applied for peer-group, all the neighbors that are part of peer-group will inherit this setting. Though the neighbor inherits the configuration from the peer-group, the neighbor-specific command, if configured, takes precedence.

This setting only takes effect after a hard reset of the session.

The **no** form of this command allows a random TCP port to be selected for the communication with the BGP neighbor.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
port <NUMBER>	Specifies a TCP port number. Range: 0 to 65535.

Examples

```
switch(config-bgp) # neighbor 1.1.1.1 port 1500  
switch(config-bgp) # no neighbor 1.1.1.1 port
```

```
switch(config-bgp) # neighbor PG port 1500
switch(config-bgp) # no neighbor PG port
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor remote-as

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} remote-as <AS-NUMBER>
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} remote-as <AS-NUMBER>
```

Description

Creates a peer, initiates the connection to the peer, and adds an entry to the BGP neighbor table. Specifies a neighbor with an autonomous system (AS) number that identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered as external. By default, neighbors that are defined using this command, exchange only unicast address prefixes.

The **no** form of this command disables the peer session and deletes the peer information.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
remote-as <AS-NUMBER>	Specifies a 4-byte AS number in asplain format (z), or asdot format (x.y), where z is a number from 1 to 4294967295 and x and y are 16-bit numbers in the range 0 to 65535.

Usage

The configured peer AS number is compared with the AS number received in the open message and a peer session is initiated only if both the AS numbers match.

Examples

```
switch(config-bgp)# neighbor 1.1.1.1 remote-as 1
switch(config-bgp)# no neighbor 1.1.1.1 remote-as 1
```

```
switch(config-bgp)# neighbor pg remote-as 1
switch(config-bgp)# no neighbor pg remote-as 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor remote as

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} remote-as <AS-no>
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} remote-as <AS-no>
```

Description

Creates an unnumbered peer and initiates the connection to the peer and adds an entry to the BGP neighbor table. This specifies a neighbor on the interface that is directly connected to the peer. This command eliminates specifying interface ip and remote-as, making BGP configuration simple and automated. The remote-as column in the bgp_neighbor table is optional for this type of peer. This command is applicable only for EBGp peers. If IBGP peers are configured via REST, the configuration is accepted, but the session is not established.

The **no** form of the command disables the peer session and deletes the peer information.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies the peer group.
remote as	Specifies the AS number as an integer value. Range: 1-

Parameter	Description
	4294967295. This is optional for BGP unnumbered.
<AS no>	Specifies the As number in dotted format. Range: 0.1-65535.65535.

Usage

This command eliminates specifying interface ip and remote-as, making BGP configuration simple and automated. The remote-as column in the bgp_neighbor table is optional for this type of peer. This command is applicable only for EBGp peers. If IBGP peers are configured via REST, the configuration is accepted, but the session is not established. BGP unnumbered is supported on IPv4, IPv6, and evpn address-family. **no ipv6 nd supress-ra** must be configured on the interface that is used for BGP unnumbered. If BGP unnumbered is configured over an SVI interface, then only the interface is expected to have the router connected to it. BGP unnumbered peering is not supported on VPNv4 address-family deployments. BGP unnumbered neighbor statistics are not displayed when the corresponding interface is not IPv6 enabled or is down. Split and subinterfaces are supported.

Examples

Creating an unnumbered peer:

```
switch(config-bgp)# neighbor 1.1.1.1 remote-as 1
```

Disabling the peer session:

```
switch(config-bgp)# no neighbor 1.1.1.1 remote-as 1
```

Creating an unnumbered peer using IPv6:

```
switch(config-bgp)# neighbor 1/1/11 remote-as 65013
```

Disabling the peer session:

```
switch(config-bgp)# no neighbor 1/1/11 remote-as 65013
```

Creating an unnumbered peer using subinterface:

```
switch(config-bgp)# neighbor 1/1/27.1 remote-as 65101
```

Disabling an unnumbered peer using subinterface:

```
switch(config-bgp)# no neighbor 1/1/27.1 remote-as 65101
```

Creating an unnumbered peer using SVI:

```
switch(config-bgp) # neighbor vlan100 remote-as 65013
```

Disabling an unnumbered peer using SVI:

```
switch(config-bgp) # no neighbor vlan100 remote-as 65013
```

Creating a peer and configuring the peer group:

```
switch(config-bgp) # neighbor pg remote-as 1
```

Disabling the peer session and peer group:

```
switch(config-bgp) # no neighbor pg remote-as 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor remove-private-AS

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} remove-private-AS  
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} remove-private-AS
```

Description

This command forces the BGP neighbor to drop the private AS numbers. When the outbound update contains a sequence of private AS numbers, this sequence is dropped. If the command is configured for peer-group, then all the neighbors that are part of peer-group will remove the private-AS before sending the BGP update message.

The **no** form of this command allows the private-AS number to be carried in BGP update message.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.

Parameter	Description
<code><IFNAME></code>	Specifies the unnumbered interface name of the neighbor.
<code><PEER-GROUP-NAME></code>	Specifies a peer group. This is not supported on BGP unnumbered.

Examples

Forcing the BGP neighbor to drop the private AS numbers:

```
switch(config-bgp)# neighbor 1.1.1.1 remove-private-AS
```

Allowing the private AS number to be carried in the BGP update message:

```
switch(config-bgp)# no neighbor 1.1.1.1 remove-private-AS
```

Forcing the BGP neighbor to drop the private AS numbers:

```
switch(config-bgp)# neighbor PG remove-private-AS
```

Allowing the private AS number to be carried in the BGP update message:

```
switch(config-bgp)# no neighbor PG remove-private-AS
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor replace-rt-asn

```
neighbor {<IP-ADDR>|<IPv6-ADDR>|<PEER-GROUP-NAME>} replace-rt-asn
no neighbor {<IP-ADDR>|<IPv6-ADDR>|<PEER-GROUP-NAME>} replace-rt-asn
```

Description

This command enables the BGP router to replace the ASN portion of the route target in the received BGP update message with the local AS number. It facilitates usage of auto RT on all BGP peers across EVPN fabrics.

This command can be used if VNIs are same across fabric and **route-target auto** is being used. When **replace-rt-asn** and a route-map with **set extcommunity rt** applied in the "IN" direction on a neighbor, **replace-rt-asn** will override the 2-byte of extended-community with local-AS.

The bgp connection must be reset using **clear bgp** to allow this configuration to take effect.

Parameter	Description
<IP-ADDR>	Specifies the neighbor's IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<IPv6-ADDR>	Specifies the neighbor's IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported for BGP unnumbered.
no	Restores default behavior.

Examples

Specifying the neighbor's IP address:

```
switch(config-bgp-l2vpn-evpn) # neighbor 1.1.1.1 replace-rt-asn
```

Specifying a peer group name:

```
switch(config-bgp-l2vpn-evpn) # neighbor PG replace-rt-asn
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor route-map

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} route-map <MAP-NAME> {in|out}
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} route-map <MAP-NAME> {in|out}
```

Description

This command applies a route map to incoming or outgoing routes. It configures the route map for modifying the default attributes of the route.



When both peer group and neighbor configuration have route maps associated, then the following configuration applies:

- For outbound route maps, peer group configuration will override the configuration of the neighbor.
- For inbound route maps, neighbor configuration will override the peer group configuration.

The **no** form of this command removes a route map.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<MAP-NAME>	Specifies the name of the route map.
in out	Sets the route map policy to apply to either the received routes from the neighbor (in) or the advertised routes to the neighbor (out).

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 route-map HPE in
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 route-map HPE in
```

```
switch(config-bgp-ipv4-uc) # neighbor PG route-map HPE in
switch(config-bgp-ipv4-uc) # no neighbor PG route-map HPE in
```

```
switch(config) # route-map Rmap permit seq 10
switch(config-route-map-Rmap-10) # match metric 100
switch(config-route-map-bgp-10) # router bgp 100
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 remote-as 100
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 route-map Rmap out
```

Configuring inbound route maps in L2VPN EVPN address family.

```
switch(config) # router bgp 100
switch(config-bgp) # neighbor 2.1.1.1 remote-as 100
```

```

switch(config-bgp)# neighbor 2.1.1.1 update-source loopback 1
switch(config-bgp)# address-family l2vpn evpn
switch(config-bgp-l2vpn-evpn)# neighbor 2.1.1.1 activate
switch(config-bgp-l2vpn-evpn)# neighbor 2.1.1.1 route-map Rmap in
switch(config-bgp-l2vpn-evpn)# neighbor 2.1.1.1 send-community extended

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-bgp-ipv4-uc	Administrators or local user group members with execution rights for this command.
9300S	config-bgp-ipv6-uc	
	config-bgp-l2vpn-evpn	

neighbor route-reflector-client

```

neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} route-reflector-client
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} route-reflector-client

```

Description

This command configures the router as a BGP route reflector and the specified peer as its client. The **no** form of this command disables this function.

Parameter	Description
<IP-ADDRESS>	Specifies the neighbor IP address in the IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or in the IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. NOTE: Pv6 MP-BGP peering must not be used for L2VPN EVPN address family, because VXLAN tunnel interface does not support IPv6 addresses.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 route-reflector-client
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 route-reflector-client
```

```
switch(config-bgp-ipv4-uc) # neighbor PG route-reflector-client
switch(config-bgp-ipv4-uc) # no neighbor PG route-reflector-client
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 1.1.1.1 route-reflector-client
switch(config-bgp-l2vpn-evpn) # no neighbor 1.1.1.1 route-reflector-client
```

```
switch(config-bgp-l2vpn-evpn) # neighbor PG route-reflector-client
switch(config-bgp-l2vpn-evpn) # no neighbor PG route-reflector-client
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 2001:0db8:85a3::8a2e:0370:7334 route-
reflector-client
switch(config-bgp-l2vpn-evpn) # no neighbor 2001:0db8:85a3::8a2e:0370:7334 route-
reflector-client
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor send-community

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} send-community [standard | extended]
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} send-community [standard | extended]
```

Description

This command allows community values to be sent to a specific neighbor. When this command is configured for the peer-group, then all the neighbors that are part of peer-group will send the community values to the peers. The parameters `standard` and `extended` send only the respective community numbers. When the command is issued without either of these parameters, both standard and extended communities will be sent to the neighbor.

The **no** form of this command will not allow the neighbor to send community values to the specific neighbors that are part of peer-group.

Parameter	Description
<code><IP-ADDR></code>	Specifies the neighbor IP address in the IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or in the IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. NOTE: IPv6 MP-BGP peering must not be used for L2VPN EVPN address family, because VXLAN tunnel interface does not support IPv6 addresses.
<code><IFNAME></code>	Specifies the unnumbered interface name of the neighbor.
<code><PEER-GROUP-NAME></code>	Specifies a peer group. This is not supported on BGP unnumbered.

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 send-community standard
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 send-community standard
```

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 send-community extended
switch(config-bgp-ipv4-uc) # no neighbor 1.1.1.1 send-community
```

```
switch(config-bgp-ipv4-uc) # neighbor PG send-community standard
switch(config-bgp-ipv4-uc) # no neighbor PG send-community standard
```

```
switch(config-bgp-ipv4-uc) # neighbor PG send-community extended
switch(config-bgp-ipv4-uc) # no neighbor PG send-community
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 1.1.1.1 send-community standard
switch(config-bgp-l2vpn-evpn) # no neighbor 1.1.1.1 send-community standard
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 1.1.1.1 send-community extended
switch(config-bgp-l2vpn-evpn) # no neighbor 1.1.1.1 send-community
```

```
switch(config-bgp-l2vpn-evpn) # neighbor PG send-community standard
switch(config-bgp-l2vpn-evpn) # no neighbor PG send-community standard
```

```
switch(config-bgp-l2vpn-evpn) # neighbor PG send-community extended
switch(config-bgp-l2vpn-evpn) # no neighbor PG send-community
```

```
switch(config-bgp-l2vpn-evpn) # neighbor 2001:0db8:85a3::8a2e:0370:7334 send-  
community extended  
switch(config-bgp-l2vpn-evpn) # no neighbor 2001:0db8:85a3::8a2e:0370:7334 send-  
community
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc config-bgp-l2vpn-evpn	Administrators or local user group members with execution rights for this command.

neighbor shutdown

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} shutdown  
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} shutdown
```

Description

This command disables the peer session, terminates any active session for the specified neighbor or peer group, and removes all associated routing information. This action can cause the sudden termination of many peering sessions.

The **no** form of this command enables the peer session for the specified neighbor.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.

Usage

Sessions are gracefully shut down when graceful-shutdown is enabled. Enter the `neighbor graceful-shutdown` command to enable graceful-shutdown. If graceful-shutdown is configured without delay or local-preference, the default values are used.

Examples

Disable the peer session, terminate any active session for the specified neighbor or peer group, and removing all associated routing information. Then enable the peer session for the specified neighbor:

```
switch(config-bgp) # neighbor 1.1.1.1 shutdown
switch(config-bgp) # no neighbor 1.1.1.1 shutdown
```

Disable the peer session, terminate any active session for the specified neighbor or peer group, and removing all associated routing information. Then enable the peer session for the specified neighbor:

```
switch(config-bgp) # neighbor pg shutdown
switch(config-bgp) # no neighbor pg shutdown
```

Establish a peer graceful shutdown:

```
switch(config-bgp) # neighbor 1.1.1.1 graceful-shutdown 10
switch(config-bgp) # neighbor 1.1.1.1 shutdown
Peer 1.1.1.1 will be shutdown in 10 seconds. Do not modify BGP configurations
until the shutdown process completes.
```

Enter an unsuccessful peer session because the gshut timer is running:

```
switch(config-bgp) # no neighbor 1.1.1.1 shutdown
Peer 1.1.1.1 is being gracefully shutdown. Peer cannot be brought up until the
shutdown process completes.
```

Enter an successful peer session because the gshut timer is running:

```
switch(config-bgp) # no neighbor pg shutdown
```

Reset the timer to the default value:

```
switch(config-bgp) # no neighbor pg graceful-shutdown 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.16	Added graceful shutdown examples and configuration.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor slow-peer

```
neighbor {<IP-ADDR>|<IPv6-ADDR>|<IFNAME>} slow-peer
no neighbor {<IPv4-ADDR>|<IPv6-ADDR>|<IFNAME>} slow-peer
```

Description

Slow peer configuration moves the peer from its normal update group to a slow update group. Removing slow peers allows the normal update group to function without being slowed down and enables faster convergence. Slow peer configuration is applicable only to explicitly configured BGP neighbors. All configured slow peers will be grouped into a slow update group. This group will converge based on the slowest group peer. Dynamic detection and splitting isn't supported. Peers can be statically configured as slow.

The **no** form of this command removes the slow peer configuration.

Parameter	Description
<IP-ADDR>	Specifies a neighbor IP address.
<IPv6-ADDR>	Specifies a neighbor IPv6 address.

Examples

Configuring a neighbor with an IP address of **1.1.1.1** as a slow peer:

```
switch(config-bgp)# neighbor 1.1.1.1 slow-peer
```

Removing the slow peer configuration for a neighbor with an IP address of **1.1.1.1**:

```
switch(config-bgp)# no neighbor 1.1.1.1 slow-peer
```

Configuring a neighbor with an IPv6 address of **2001::2** as a slow peer:

```
switch(config-bgp)# neighbor 2001::2 slow-peer
```

Removing the slow peer configuration for a neighbor with an IPv6 address of **2001::2**:

```
switch(config-bgp)# no neighbor 2001::2 slow-peer
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor soft-reconfiguration inbound

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} soft-reconfiguration inbound
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} soft-reconfiguration inbound
```

Description

This command enables you to generate inbound updates from a neighbor and change and activate BGP policies without clearing the BGP session. Changes in BGP policies require the BGP session to be cleared which can have a large negative impact on network operations.

The **no** form of this command disables this setting.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.

Usage

- To perform inbound soft reconfiguration, the BGP speaker must store all received route updates, regardless of the current inbound policy.
- When inbound soft reconfiguration is enabled, the stored updates are processed by the new policy configuration to create new inbound updates.

Examples

```
switch(config-bgp-ipv4-uc) # neighbor 1.1.1.1 soft-reconfiguration inbound
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-bgp-ipv4-uc	Administrators or local user group members with execution rights for this command.
9300S	config-bgp-ipv6-uc	

neighbor timers

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} timers <KEEPALIVE> <HOLDTIME>
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} timers <KEEPALIVE> <HOLDTIME>
```

Description

This command sets the timers for a specific BGP neighbor or peer group. When the timer is applied to peer-group then all the neighbors that are part of peer-group will inherit the value configured.

The **no** form of this command clears the timers for a specific BGP neighbor or peer group.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<KEEPALIVE>	Specifies the Keep-Alive timer value for the neighbor. Default: 60 seconds. Range: 0-65535.
<HOLDTIME>	Specifies the Hold-timer value. Default: 180 seconds. Range: 0-65535.

Examples

```
switch(config-bgp)# neighbor 1.1.1.1 timers 120 360
switch(config-bgp)# no neighbor 1.1.1.1 timers 120 360
```

```
switch(config-bgp)# neighbor pg timers 120 360
switch(config-bgp)# no neighbor pg timers 120 360
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor timers connect-retry

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} timers connect-retry <RETRYTIME>
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} timers connect-retry <RETRYTIME>
```

Description

This command sets the connect-retry timer for a specific BGP neighbor or peer group.

The **no** form of this command clears the connect-retry timers for a specific BGP neighbor or peer group.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<RETRYTIME>	Specifies the retry timer value.

Usage

When the timer is applied to peer-group, then all the neighbors that are part of peer-group inherit the value configured. A connect-retry timer configured for a specific peer takes precedence over that configured for the peer group of this peer. In addition, a connect-retry timer configured for a specific peer or peer group takes precedence over that configured on the global level.

Examples

Setting the connect-retry timer to 50:

```
switch(config-bgp)# neighbor 1.1.1.1 timers connect-retry 50
```

Removing the connect-retry timer:

```
switch(config-bgp)# no neighbor 1.1.1.1 timers connect-retry 50
```

Setting the connect-retry timer to 80:

```
switch(config-bgp) # neighbor pg timers connect-retry 80
```

Removing the connect-retry timer:

```
switch(config-bgp) # no neighbor pg timers connect-retry 80
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor ttl-security-hops

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} ttl-security-hops <HOP-COUNT>  
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} ttl-security-hops <HOP-COUNT>
```

Description

This command enables BGP to establish connection with external peers residing on networks that are not directly connected. By enabling this feature, the received TTL from a BGP peer is compared with the difference "255 - hop-count". BGP messages coming with a TTL less than this value are not accepted. BGP peering will not be established if the TTL in the session establishment is received with a lower value. Also, by enabling this feature the router will send BGP packets with TTL value of 255 to the neighbor. For a neighbor, either TTL security or `ebgp-multihop` can be configured, not both together. If there are multiple paths to reach the node, then the hop count should be configured considering the longest route.

The **no** form of this command disables the peer ttl-security-hop feature.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<HOP-COUNT>	Specifies the hop count to reach the neighbor for the eBGP session. Range: 1-255.

Examples

```
switch(config-bgp)# neighbor 1.1.1.1 ttl-security-hops 10  
switch(config-bgp)# no neighbor 1.1.1.1 ttl-security-hops
```

```
switch(config-bgp)# neighbor pg ttl-security-hops 5  
switch(config-bgp)# no neighbor pg ttl-security-hops
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor update-source

```
neighbor {<IP-ADDRESS>|<PEER-GROUP-NAME>}  
    update-source {<IPv4>|<IPv6> | loopback <NUMBER>}  
no neighbor {<IP-ADDRESS>|<PEER-GROUP-NAME>}  
    update-source [<IPv4>|<IPv6> | loopback <NUMBER>]
```

Description

This command specifies the source address to reach the neighbor.

An iBGP connection can occur as long as there is a TCP/IP path between the routers. If multiple paths exist between the iBGP routers, using a loopback interface as the neighbor address can add stability to the network. With this command, stability can be achieved by providing the loopback interface address as the source address of the TCP/IP session.

The **no** form of this command negates the route updates of the neighbor.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
<PEER-GROUP-NAME>	Specifies a peer group.
<IPv4>	Specifies an interface by IPv4 address.
<IPv6>	Specifies an interface by IPv6 address.
loopback <NUMBER>	Specifies a loopback interface number.

Examples

```
switch(config-bgp)# neighbor 1.1.1.1 update-source loopback 1  
switch(config-bgp)# no neighbor 1.1.1.1 update-source
```

```
switch(config-bgp)# neighbor PG update-source loopback 1  
switch(config-bgp)# no neighbor PG update-source
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

neighbor weight

```
neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} weight <WEIGHT-VALUE>  
no neighbor {<IP-ADDR>|<IFNAME>|<PEER-GROUP-NAME>} weight <WEIGHT-VALUE>
```

Description

This command assigns a weight to a neighbor connection. When the weight is applied to a peer-group then all the neighbors that are part of the peer-group will inherit the value configured.

The **no** form of this command removes a weight assignment.

Parameter	Description
<IP-ADDR>	Specifies an IP address.
<IFNAME>	Specifies the unnumbered interface name of the neighbor.
<PEER-GROUP-NAME>	Specifies a peer group. This is not supported on BGP unnumbered.
<WEIGHT-VALUE>	Specifies the weigh to be associated with the routes received from the neighbor. Range: 0-65535.

Examples

```
switch(config-bgp)# neighbor 1.1.1.1 weight 500  
switch(config-bgp)# no neighbor 1.1.1.1 weight
```

```
switch(config-bgp)# neighbor pg weight 600
switch(config-bgp)# no neighbor pg weight
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Added support for BGP unnumbered.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp	Administrators or local user group members with execution rights for this command.

network

```
network {[<IPV4/MASK> | <IPV6/MASK>]} [route-map <ROUTE-MAP-NAME>]
no network {[<IPV4/MASK> | <IPV6/MASK>]} [route-map <ROUTE-MAP-NAME>]
```

Description

This command specifies the networks to be advertised by the Border Gateway Protocol (BGP) routing processes.

The **no** form of this command removes an entry from the routing table.

Parameter	Description
<IPV4/MASK>	Specifies the IPv4 network with mask. For example: 1.1.1.1/24
<IPV6/MASK>	Specifies the IPv6 network with mask. For example: 2001:0db8:85a3::8a2e:0370:7334/24
route-map <ROUTE-MAP-NAME>	Optional parameter. Specifies a route map to apply to the prefixes advertised by this specific network statement.

Usage

- This command is used to advertise prefixes currently installed in the routing table into the BGP table.
- Use the `route-map` keyword to apply the specified route map to network advertisements. The mask length as configured in the network statement must match the mask length of prefixes in the routing table.

Examples

```
switch(config-bgp-ipv4-uc) # network 11.11.11.0/24  
switch(config-bgp-ipv4-uc) # no network 11.11.11.0/24
```

```
switch(config-bgp-ipv6-uc) # network 2001:0db8:85a3::8a2e:0370:7334/24  
switch(config-bgp-ipv6-uc) # no network 2001:0db8:85a3::8a2e:0370:7334/24
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute {connected|ospf <process ID> |host-routes|static|local loopback} [route-map  
<ROUTE-MAP-NAME>]  
no redistribute {connected|ospf <process ID> |host-routes|static|local loopback} [route-  
map <ROUTE-MAP-NAME>]
```

Description

This command specifies routes to import into BGP. This command causes routes from the specified protocol to be considered for redistribution into BGP.

The **no** form of this command specifies no redistribution into BGP.

Parameter	Description
connected	Redistributes directly attached networks (directly attached to the subnet or host).
host-routes	Redistributes ARP entries. ARP entries learned through EVPN or over VXLAN tunnels are not redistributed.
ospf	Redistributes Open Shortest Path First (OSPFv2) routes. It is optional to mention the process ID. Range: <1-65535>
static	Redistributes statically configured routes .
local loopback	Performs the following functions:

Parameter	Description
	- Redistributes local routes on loopback interfaces. - For EVPN enabled VRFs, it advertises the IP address of loopback interfaces as a EVPN Type-5 prefix route.
<code>route-map <ROUTE-MAP-NAME></code>	Optional. Specifies a route map to match for redistribution.

Usage

- If a route map is specified, then routes that pass the match clause specified in the route map will be imported into the BGP peer Routing Information Base (RIB).
- Route-maps must be configured prior to being referenced in redistribution statements.
- Redistribute connected is required to redistribute connected subnet even if redistribute local loopback is already configured.

Examples

Redistribute directly attached networks:

```
switch(config-bgp-ipv4-uc) # redistribute connected
switch(config-bgp-ipv4-uc) # no redistribute connected
```

Redistributing local routes on loopback interfaces:

```
switch(config-bgp-ipv4-uc) # redistribute local loopback
switch(config-bgp-ipv4-uc) # no redistribute local loopback
```

Redistributing ARP entries:

```
switch(config-bgp-ipv4-uc) # redistribute host-routes route-map map1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.13	Added route-map support for host-routes .
10.12	Added support for the <code>host-routes</code> parameter.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-bgp-ipv4-uc config-bgp-ipv6-uc	Administrators or local user group members with execution rights for this command.

router bgp

```
router bgp <AS-NUMBER>
no router bgp <AS-NUMBER>
```

Description

This command configures the BGP instance on the router, configures the AS (Autonomous System) the router belongs to, and enters into the BGP router configuration mode. Only a single BGP AS number can be assigned for the entire system.

The **no** form of the command deletes the BGP instance from the router.

Parameter	Description
<i>AS-NUMBER</i>	Specifies a 4-byte AS number in the range 1-4294967295 in integer format or from 0.1-65535.65535 in dotted format.

Examples

Configuring the BGP instance with the AS number:

```
switch(config)# router bgp 100
```

Deleting BGP configurations:

```
switch(config)# no router bgp 100
This will delete all BGP configurations on this device.
Continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show bgp

```
show bgp [{vrf <VRF-NAME>|all-vrf}] [{ipv4 unicast|ipv6 unicast  
|all}] [vsx-peer][update-group [<INDEX>]]  
show bgp l2vpn evpn
```

Description

This command shows entries in the BGP routing table.

Parameter	Description
ipv4	Selects the IPv4 address family.
ipv6	Selects the IPv6 address family.
unicast	The subaddress family identifier.
vrf <VRF-NAME>	Select to display information by VRFs by specifying the VRF name.
all-vrf	Select to display the BGP summary information for all VRFs and address-families.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.
update-group [<INDEX>]	Select to display information about update-group and peers which are member of that update-group for given afi/safi. Specifying an integer defines the desired update-group index.

Examples

Showing BGP routing table information for VRF 1 IPv4 unicast:

```
switch# show bgp vrf v1 ipv4 unicast  
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,  
               i internal, e external S Stale, R Removed, a additional-paths  
Origin codes: i - IGP, e - EGP, ? - incomplete  
  
VRF : v1  
Local Router-ID 9.0.0.1  
  
      Network          Nexthop      Metric    LocPrf    Weight Path  
-----  
*>e 9.0.0.0/24         9.0.0.2        0         100       0      65534.65535 3.4  
18.54934 3574.8570 5.6 ?  
*>e 100.0.0.0/24       9.0.0.2        0         100       0      200 ?  
*>e 100.0.1.0/24       9.0.0.2        0         100       0      200 ?  
*>e 100.0.2.0/24       9.0.0.2        0         100       0      200 ?  
*>e 100.0.3.0/24       9.0.0.2        0         100       0      200 ?  
*ae 100.0.3.0/24       9.0.0.3        0         100       0      200 ?  
Total number of entries 6
```

Showing BGP routing table information for L2VPN EVPN:

```
switch# show bgp l2vpn evpn
```

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, e external S Stale, R Removed

Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]

EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]

VRF : default

Router-ID not configured

Network	Nexthop
Metric LocPrf Weight Path	

Route Distinguisher: 10.1.1.54:32967 (L2VNI 30000)	
*> [2]:[0]:[0]:[00:06:f6:3f:e3:c1]:[] 100 32768 i	1.1.1.20 0
*> [2]:[0]:[0]:[8c:60:4f:f2:f5:41]:[] 100 0 i	1.1.1.10 0
*> [3]:[0]:[1.1.1.1] 100 0 ?	0.0.0.0 0
Total number of entries 3	

```
switch# show bgp l2vpn evpn neighbors 1920:1680:1:1::8
```

Codes: ^ Inherited from peer-group, * Dynamic Neighbor

VRF : default

BGP Neighbor 1920:1680:1:1::8 (Internal)

Description	: RR peer-group^		
Peer-group	: RRv6		
Remote Router Id	: 192.168.1.8	Local Router Id	: 192.168.1.1
Remote AS	: 65001	Local AS	: 65001
Remote Port	: 42423	Local Port	: 179
State	: Established	Admin Status	: Up
Conn. Established	: 5	Conn. Dropped	: 4
Passive	: No	Update-Source	: loopback0^
Cfg. Hold Time	: 180	Cfg. Keep Alive	: 60
Neg. Hold Time	: 180	Neg. Keep Alive	: 60
Up/Down Time	: 06h:46m:13s	Connect-Retry Time	: 120
Local-AS Prepend	: No	Alt. Local-AS	: 0
BFD	: Disabled	Slow Peer	: Yes
Password	:		
Last Err Sent	: No Error		
Last SubErr Sent	: No Error		
Last Err Rcvd	: No Error		
Last SubErr Rcvd	: No Error		
Graceful-Restart	: Enabled	Gr. Restart Time	: 120
Gr. Stalepath Time	: 300	Remove Private-AS	: No
TTL	: 255	Local Cluster-ID	:
Weight	: 0	Fall-over	: No
Confederation-Peers	: No		

Message statistics	Sent	Rcvd
-----	----	-----
Open	8	7
Notification	3	1
Updates	20730	91332
Keepalives	1153	952
Route Refresh	0	0
Total	21894	92292

Capability	Advertised	Received
Route Refresh	Yes	Yes
Graceful Restart	Yes	Yes
Add-Path	No	No
Four Octet ASN	Yes	Yes
Address family IPv4 Unicast	No	No
Address family IPv6 Unicast	No	No
Address family VPNv4 Unicast	No	No
Address family L2VPN EVPN	Yes	Yes
Address Family : L2VPN EVPN		


```

Rt. Reflect. Client : No
Allow-AS in       : 0
Max. Prefix       : 64000
Nexthop-Self      :
Cfg. Add-Path     :
Neg. Add-Path     :
Routemap In       :
Routemap Out      :
ORF type          : Prefix-list
ORF capability     :
Send Community    : extended^
Advt. Interval    : 30
Soft Reconfig In  :
Default-Originate :

```

Showing all BGP update groups:

```

switch# show bgp all update-group

VRF : default

BGP Update-Group 1
  Address Family : ipv4-unicast
  Peer Count     : 5
  Peering Type   : internal
  Slow Group     : No

  Members
  -----
  110.162.100.221, 120.221.221.221, 130.121.21.111, 140.131.131.131,
  150.100.101.2

BGP Update-Group 2
  Address Family : ipv4-unicast
  Peer Count     : 2
  Peering Type   : external
  Slow Group     : Yes

  Members
  -----
  20.1.1.1, 30.1.1.1

BGP Update-Group 3
  Address Family : ipv6-unicast
  Peer Count     : 1
  Peering Type   : external
  Slow Group     : No

  Members
  -----
  20ab::cd:08

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Replaced IPv4 with IP in commands. IPv4 is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp

```
show bgp
[vrf <VRF-NAME>] {ipv4 unicast <A.B.C.D/M>}|{ipv6 unicast <X::Y/M>}
[vsx-peer]
l2vpn evpn
  EVPN Route-Type 1 prefix: [1]:[ESI]:[EthTag]
  RD-[ROUTE_TYPE]:[ESI]:[EthTag]:[MAC]:[OrigIP]
  RD-[ROUTE_TYPE]:[EthTag]:[OrigIP]
  RD-[ROUTE_TYPE]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
```

Description

This command displays entries in the BGP routing table that are part of the specified network. For EVPN Route-type 2 with MAC only prefix as an input, displays all the prefixes containing the specific MAC address (MAC route, MAC/IP route, Host route).

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast <A.B.C.D/M>	Shows the information for an IPv4 unicast family with an IP prefix (network/length such as 35.0.0.0/8) in the BGP routing table to display.
ipv6 unicast <X::Y/M>	Shows the information for an IPv6 unicast family an IPv6 prefix in the BGP routing table to display.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.
RD-[ROUTE_TYPE]:[ESI]:[EthTag]:[MAC]:[OrigIP]	EVPN Route-Type 2 prefix.

Parameter	Description
RD-[ROUTE_TYPE]:[EthTag]:[OrigIP]	EVPN Route-Type 3 prefix.
RD-[ROUTE_TYPE]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]	EVPN Route-Type 5 prefix.

Examples

Showing the entries in the BGP routing table that are part of an IPv4 unicast network

```
switch# show bgp ipv4 unicast 10.0.0.0/16

VRF : default
BGP Local AS 2          BGP Router-ID 1.1.1.2

Network      : 10.0.0.0/16      Nexthop      : 1.1.1.1
Peer         : 1.1.1.1         Origin       : IGP
Metric       : 0               Local Pref   : 100
Weight       : 0               Calc. Local Pref : 100
Best         : Yes             Valid        : Yes
Type         : external        Stale        : No
Originator ID : 0.0.0.0        Path ID      : 0
Aggregator ID :
Aggregator AS :
Atomic Aggregate :
RFD Flaps    : 0               RFD Penalty  : 0

AS-Path      : 1
Cluster List :
Communities  :
50:100,50:101,50:102,50:103,50:104,50:105,50:106,50:107,50:108,50:109,50:110,50:1
Extd. Communities :
```

Showing the entries in the BGP routing table that are part of L2VPN EVPN

```
switch# show bgp l2vpn evpn vni 30000
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]

VRF : default
Router-ID not configured

      Network                                     Nexthop
Metric LocPrf Weight Path
-----
Route Distinguisher: 10.1.1.54:32967      (L2VNI 30000)
*>   [2]:[0]:[0]:[00:06:f6:3f:e3:c1]:[]    1.1.1.20      0
    100    32768    i
*>   [2]:[0]:[0]:[8c:60:4f:f2:f5:41]:[]    1.1.1.10      0
    100     0      i
*>   [3]:[0]:[1.1.1.1]                    0.0.0.0       0
    100     0      ?
Total number of entries 3
```

Showing the entries in the BGP routing table for EVPN route-type 2

```

switch# show bgp l2vpn evpn 2:2-[2]:[0]:[0]:[00:50:56:96:6d:6f]:[20.20.1.10]
VRF : default
BGP Local AS 1          BGP Router-id 3.3.3.3
Network                 : 2:2-[2]:[0]:[0]:[00:50:56:96:6d:6f]:[20.20.1.10]
Nexthop                 : 1.1.1.1
vni                     : 2                      vni_type           : L2VNI
Peer                    : 2.2.2.2                Origin              : incomplete
Metric                  : 0                      Local Pref          : 100
Weight                  : 0                      Calc. Local Pref    : 100
Best                    : Yes                    Valid               : Yes
Type                    : internal               Stale               : No
Originator ID           : 1.1.1.1               Aggregator ID       :
Aggregator AS           :
Atomic Aggregate        :
AS-Path                 :
Cluster List            :
Communities             :
Ext-Communities         : RT: 2:2 RT: 10:10 Router MAC: 00:00:00:00:00:11
Network                 : 2:2-[2]:[0]:[0]:[00:50:56:96:6d:6f]:[20.20.1.10]
Nexthop                 : 1.1.1.1
vni                     : 10000                  vni_type           : L3VNI
Peer                    : 2.2.2.2                Origin              : incomplete
Metric                  : 0                      Local Pref          : 100
Weight                  : 0                      Calc. Local Pref    : 100
Best                    : Yes                    Valid               : Yes
Type                    : internal               Stale               : No
Originator ID           : 1.1.1.1               Aggregator ID       :
Aggregator AS           :
Atomic Aggregate        :
AS-Path                 :
Cluster List            :
Communities             :
Ext-Communities         : RT: 2:2 RT: 10:10 Router MAC: 00:00:00:00:00:11

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Replaced IPv4 with IP in commands. IPv4 is deprecated.
10.08	Added l2vpn evpn route types
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp community


```
show bgp [{ipv4 | ipv6 | ipv4 {vrf <VRF-NAME>}} unicast] community [<VALUE> | <TYPE>]
[vsx-peer]
```

Description

This command shows routes that belong to BGP communities. Optionally you can specify displaying information by a specific community or by VRF.

Parameter	Description
ipv4	Shows the information for an IPv4 address family.
ipv6	Shows the information for an IPv6 address family.
unicast	Shows the information for a subaddress family identifier.
ipv4 vrf <VRF-NAME>	Shows the information for a specified VRF.
<VALUE>	Shows the information for a community number. Specify the information in aa:nn format.
<TYPE>	Shows a specified community type. Select the following well-known communities, as well as others: internet Advertise the prefix to all BGP neighbors. local-as Do not advertise the prefix outside the sub-AS. no-advertise Do not advertise the prefix to any BGP neighbors. no-export Do not advertise the prefix to any eBGP neighbors.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for routes that belong to all BGP communities:

```
switch# show bgp ipv4 unicast community
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath, i
internal, e external S Stale, R Removed, a additional-paths VRF : default Local
Router-ID 9.0.0.1
Network                Nexthop      Metric    LocPrf    Weight Path
-----
*>e 9.0.0.0/24          9.0.0.2      0         100       0       200 ?
*>e 100.0.0.0/24        9.0.0.2      0         100       0       200 ?
*>e 100.0.1.0/24        9.0.0.2      0         100       0       200 ?
*>e 100.0.2.0/24        9.0.0.2      0         100       0       200 ?
*>e 100.0.3.0/24        9.0.0.2      0         100       0       200 ?
*ae 100.0.3.0/24       9.0.0.3      0         100       0       200 ?
Total number of entries 6
```

Showing information for routes that belong to the 200:20 BGP community number:

```
switch# show bgp ipv4 unicast community 200:20
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, e external S Stale, R RemovedOrigin codes: i - IGP, e - EGP, ? -
incomplete
VRF : defaultLocal Router-ID 9.0.0.1
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	100	0	200 ?
*ae 100.0.3.0/24	9.0.0.3	0	100	0	200 ?

Total number of entries 6

Showing information for routes that belong to the Internet BGP community type:

```
switch# show bgp ipv4 unicast community internet
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete
VRF : default
Local Router-ID 9.0.0.1
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	100	0	200 ?
*ae 100.0.3.0/24	9.0.0.3	0	100	0	200 ?

Total number of entries 6

Showing information for routes that belong to the local-as BGP community type:

```
switch# show bgp ipv4 unicast community local-as
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete
VRF : default

Local Router-ID 9.0.0.1
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	100	0	200 ?
*ae 100.0.3.0/24	9.0.0.3	0	100	0	200 ?

Total number of entries 6

Showing information for routes that belong to the no-advertise BGP community type:

```

switch# show bgp ipv4 unicast community no-advertise
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, e external S Stale, R Removed, a additional-paths Origin codes: i -
IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 9.0.0.1

```

Network	Nextthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	100	0	200 ?
*ae 100.0.3.0/24	9.0.0.2	0	100	0	200 ?

```

Total number of entries 6

```

Showing information for routes that belong to the no-export BGP community type:

```

switch# show bgp ipv4 unicast community no-export
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath, i
internal, e external S Stale, R Removed, a additional-paths Origin codes: i - IGP,
e - EGP, ? - incomplete

VRF : default
Local Router-ID 9.0.0.1

```

Network	Nextthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	100	0	200 ?
*ae 100.0.3.0/24	9.0.0.3	0	100	0	200 ?

```

Total number of entries 6

```

Showing information for routes that belong to the gshut BGP community type:

```

switch# show bgp ipv4 unicast community gshut
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
i internal, e external S Stale, R Removed Origin codes: i - IGP, e - EGP, ? -
incomplete

VRF : default
Local Router-ID 1.1.1.2

```

Network	Nextthop	Metric	LocPrf	Weight	Path
*>e 1.1.1.0/24	10.1.1.2	0	0	0	2 i

```

Total number of entries 1

switch#
switch# show bgp ipv6 unicast community gshut

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath, i
internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```
VRF : default
Local Router-ID 1.1.1.2
```

Network	Nexthop	Metric	LocPrf	Weight	Path

*>e 1::/64	10::2				
fe80::98f2:b300:1368:e882		0	0	0	2 i
Total number of entries 1					



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp flap-statistics

```
show bgp {vrf <VRF_NAME> | all-vrf} [{ipv4 unicast | ipv6 unicast | all}] flap-statistics
```

Description

Displays all the flapped and suppressed routes.

Usage

Status of the route with dampening enabled:

- If the route is available, the history flag is unset.
- If route has been flapping, is not suppressed and is withdrawn; the state of the route is **h**
- If route is currently available but is suppressed due to dampening, the state of the route is **d**
- If the route is unsuppressed and currently withdrawn, the state of the route is **h**

Examples

Showing all the flapped and suppressed routes:

```
switch# show bgp all
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```

VRF : default
Local Router-ID 1.1.1.1

Address-family : IPv4 Unicast
-----
      Network          Nexthop          Metric      LocPrf      Weight Path
*>i 2.2.2.0/24          2.2.2.2            0           100         0         ?
*>i 11.1.1.0/24         2.2.2.2            0           100         0         ?
*ai 11.1.1.0/24         2.2.2.3            0           100         0         ?
Total number of entries 3

Address-family : IPv6 Unicast
-----
      Network          Nexthop          Metric      LocPrf      Weight Path
Total number of entries 0

```

```

switch# show bgp ipv4 unicast flap-statistics
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 20.0.0.1

      Network          Nexthop          Flaps          Reuse          Path
*>e 2.2.2.0/24          20.0.0.2          1              00h:00m:00s    300 ?
de 3.3.3.0/24          20.0.0.2          2              00h:29m:31s    300 ?
Total number of entries 2

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp neighbor advertised-routes

```

show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast
    | l2vpn evpn | all} neighbors <IP-ADDRESS>
    advertised-routes [vsx-peer]
show bgp l2vpn evpn neighbors <IP-ADDRESS> advertised-routes

```

Description

Shows all routes that have been advertised to the specified neighbor.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
l2vpn evpn	Shows the information for L2VPN EVPN address family.
all	Shows the information for all address families and subaddress families.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
<IP-ADDRESS>	Shows the information for a neighbor IP address.

Examples

Showing routes that have been advertised to the specified IPv4 unicast neighbor:

```
switch# show bgp ipv4 unicast neighbors 9.0.0.1 advertised-routes
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 9.0.0.2
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	0	0	200 65534.65535
3.4 18.54934 3574.8570 5.6 ?					
*>e 100.0.0.0/24	9.0.0.2	0	0	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	0	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	0	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	0	0	200 ?

```
Total number of entries 5
```

Showing routes that have been advertised to the specified L2VPN EVPN neighbor:

```
switch# show bgp l2vpn evpn neighbor 9.0.0.1 advertised-routes
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]

VRF : default
Local Router-ID 9.0.0.2
```

Network	Nexthop	Metric
LocPrf Weight Path		


```

Route Distinguisher: 10.1.1.54:32967      (L2VNI 30000)
*> [2]:[0]:[0]:[00:06:f6:3f:e3:c1]:[]      1.1.1.20      0      100
    32768 i
*> [2]:[0]:[0]:[8c:60:4f:f2:f5:41]:[]      1.1.1.10      0      100
    0 i
Total number of entries 2

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp neighbor paths

```

show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast
    | all} neighbors <IP-ADDRESS> paths [vsx-peer]
show bgp l2vpn evpn neighbors <IP-ADDRESS> paths

```

Description

Shows autonomous system paths learned from the specified neighbor.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
<IP-ADDRESS>	Shows the information for a neighbor IP address.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.

Examples

Showing autonomous system paths learned from the specified IPv4 unicast neighbor:

```
switch# show bgp ipv4 unicast neighbors 192.168.12.2 paths
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
VRF : default
Local Router-ID 9.0.0.1

  Network                Nexthop                Path
  -----
*>e 9.0.0.0/24            9.0.0.2                200 65534.65535 3.4 18.54934 3574.8570 5.6
*>e 100.0.0.0/24          9.0.0.2                200
*>e 100.0.1.0/24          9.0.0.2                200
*>e 100.0.2.0/24          9.0.0.2                200
*>e 100.0.3.0/24          9.0.0.2                200
Total number of entries 5
```

Showing autonomous system paths learned from the specified L2VPN EVPN neighbor:

```
switch# show bgp l2vpn evpn neighbors 192.168.12.1 paths

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]

VRF : default
Local Router-ID 9.0.0.2

  Network                Nexthop                Path
  -----
-
Route Distinguisher: 10.1.1.54:32967 (L2VNI 30000)
*> [2]:[0]:[0]:[00:06:f6:3f:e3:c1]:[] 1.1.1.20                100
*> [2]:[0]:[0]:[8c:60:4f:f2:f5:41]:[] 1.1.1.10                100
Total number of entries 2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp neighbor received orf-prefix-list


```
show bgp [vrf <VRF-NAME>]{ipv4 unicast | ipv6 unicast | all} neighbors <IP-ADDRESS>
received orf-prefix-list
```

Description

Shows all the prefix lists received from the specified neighbor.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
<IP-ADDRESS>	Shows the information for a neighbor IP address.

Examples

Showing received prefix list from the specified neighbor:

```
switch# show bgp ipv4 unicast neighbors A.B.C.D received orf-prefix-list
Address family: IPv4 Unicast

ip prefix-list 10.0.0.200: 4 entries

  seq 10 permit 28.119.16.0/24

  seq 15 deny 28.119.19.0/24

  seq 20 permit 28.119.17.0/24

Address family: IPv6 Unicast

ip prefix-list 10.0.0.200: 4 entries

  seq 30 permit 2000::/64

  seq 35 deny 3000::/64

  seq 40 permit 4000:0/64
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp neighbor received-routes

```
show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast
    | all} neighbors <IP-ADDRESS> received-routes [vsx-peer]
show bgp l2vpn evpn neighbors <IP-ADDRESS> received-routes
```

Description

Shows received routes from the specified neighbor.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
<IP-ADDRESS>	Shows the information for a neighbor IP address.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.

Examples

Showing received routes from the specified IPv4 unicast neighbor:

```
switch# show bgp ipv4 unicast neighbors 192.168.12.1 received-routes
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 9.0.0.2
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	0	0	200 65534.65535
3.4 18.54934 3574.8570	5.6 ?				
*>e 100.0.0.0/24	9.0.0.2	0	0	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	0	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	0	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	0	0	200 ?
*ae 100.0.3.0/24	9.0.0.2	0	0	0	200 ?

```
Total number of entries 6
```

Showing received routes from the specified L2VPN EVPN neighbor:

```
switch# show bgp l2vpn evpn neighbors 192.168.12.1 received-routes

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]

VRF : default
Local Router-ID 9.0.0.2

      Network
LocPrf Weight Path
-----
Route Distinguisher: 10.1.1.54:32967 (L2VNI 30000)
*> [2]:[0]:[0]:[00:06:f6:3f:e3:c1]:[] 1.1.1.20 0 100
  32768 i
*> [2]:[0]:[0]:[8c:60:4f:f2:f5:41]:[] 1.1.1.10 0 100
  0 i
Total number of entries 2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp neighbor routes

```
show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast
| all} neighbors <IP-ADDRESS> routes [vsx-peer]
show bgp l2vpn evpn neighbors <IP-ADDRESS>
```

Description

This command shows routes that are received and accepted from the specified neighbor.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.

Parameter	Description
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
<IP-ADDRESS>	Shows the information for a neighbor IP address.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.

Examples

Showing all routes that are received and accepted from the specified neighbor:

```
switch# show bgp ipv4 unicast neighbors 9.0.0.2 routes
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 9.0.0.1
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	100	0	200 65534.65535
3.4 18.54934 3574.8570 5.6 ?					
*>e 100.0.0.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.1.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.2.0/24	9.0.0.2	0	100	0	200 ?
*>e 100.0.3.0/24	9.0.0.2	0	100	0	200 ?
*ae 100.0.3.0/24	9.0.0.3	0	100	0	200 ?

Total number of entries 6

Showing 12 VPN EVPN routes that are received and accepted from the specified neighbor:

```
switch# show bgp l2vpn evpn neighbor 9.0.0.2 routes

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]

VRF : default
Local Router-id: 9.0.0.1
```

Network	Nexthop	Metric	LocPrf	Weight	Path
*>e 9.0.0.0/24	9.0.0.2	0	0	0	200 65534.65535
3.4 18.54934 3574.8570 5.6 ?					
*>e 100.0.0.0/24	9.0.0.2	0	0	0	200 ?

```
*>e 100.0.1.0/24      9.0.0.2      0      0      0      200 ?
*>e 100.0.2.0/24      9.0.0.2      0      0      0      200 ?
*>e 100.0.3.0/24      9.0.0.2      0      0      0      200 ?
*ae 100.0.3.0/24      9.0.0.3      0      100    0      200 ?
Total number of entries 6
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp neighbors

```
show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast | all}
    neighbors [vsx-peer]
show bgp l2vpn evpn neighbors
```

Description

This command shows information about BGP and TCP connections to neighbors. If neighbors are member of a peer-group, the command shows the configured values inherited from the peer-group. The configured values are postfixed with a caret (^) for inherited values.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.

Examples

Showing all information about BGP and TCP connections to neighbors:

```

switch# show bgp all neighbors
Codes: ^ Inherited from peer-group
VRF : default

BGP Neighbor 10.1.1.2 (Internal)
  Description      :
  Peer-group       :

  Remote Router Id : 10.1.1.2      Local Router Id : 1.0.0.1
  Remote AS        : 1            Local AS         : 1
  Remote Port      : 0            Local Port       : 0
  State            : Established   Admin Status     : Up
  Conn. Established : 1            Conn. Dropped    : 0
  Passive          : No           Update-Source    :
  Cfg. Hold Time   : 180          Cfg. Keep Alive  : 60
  Neg. Hold Time   : 0            Neg. Keep Alive  : 0
  Up/Down Time     : 00h:00m:00s  Connect-Retry Time : 120
  Local-AS Prepend : No           Alt. Local-AS    : 0
  BFD              : Disabled     Slow Peer        : No
  Password         :
  Last Err Sent    : No Error
  Last SubErr Sent : No Error
  Last Err Rcvd    : No Error
  Last SubErr Rcvd : No Error

  Graceful-Restart : Enabled       Gr. Restart Time : 120
  Gr. Stalepath Time : 150         Remove Private-AS : No
  TTL               : 255          Local Cluster-ID  :
  Weight            : 0            Fall-over         : No

  Message statistics      Sent      Rcvd
  -----
  Open                    7          6
  Notification            5          2
  Updates                 3          2
  Keepalives             12         10
  Route Refresh           0          0
  Total                   28         20

  Capability              Advertised  Received
  -----
  Route Refresh           Yes         No
  Graceful Restart        Yes         No
  Four Octet ASN          Yes         No
  Add-Path                Yes         Yes
  Address family IPv4 Unicast Yes         No
  Address family IPv6 Unicast No         No
  Address family L2VPN EVPN No         No

  Address Family : IPv4 Unicast
  -----
  Rt. Reflect. Client : No          Send Community    :
  Allow-AS in         : 0           Advt. Interval    : 30
  Max. Prefix         : 64000       Soft Reconfig In  :
  Nexthop-Self        :             Default-Originate :
  Update-Group        : 2

  Cfg. Add-Path        : Send and Receive
  Neg. Add-Path        : Send and Receive
  Routemap In          :
  Routemap Out         :

```

ORF type : Prefix-list
ORF capability : Receive

Address Family : IPv6 Unicast

Rt. Reflect. Client : No Send Community :
Allow-AS in : 0 Advt. Interval : 30
Max. Prefix : 64000 Soft Reconfig In :
Nexthop-Self : Default-Originate :
Update-Group : 3

Cfg. Add-Path : Send and Receive
Neg. Add-Path : Send and Receive
Routemap In :
Routemap Out :
ORF type : Prefix-list
ORF capability : Receive

Address Family : L2VPN EVPN

Rt. Reflect. Client : No Send Community : extended
Allow-AS in : 0 Advt. Interval : 30
Max. Prefix : 32768 Soft Reconfig In :
Nexthop-Self : Default-Originate :
Update-Group : 4

Cfg. Add-Path :
Neg. Add-Path :
Routemap In :
Routemap Out :
ORF type : Prefix-list
ORF capability : Receive

Showing information about L2VPN EVPN connections to neighbors:

switch# **show bgp l2vpn evpn neighbors**

Codes: ^ Inherited from peer-group, * Dynamic Neighbor

VRF : default

BGP Neighbor 10.1.1.2 (Internal)

Description :
Peer-group :

Remote Router Id : 10.1.1.2 Local Router Id : 10.1.1.1
Remote AS : 1 Local AS : 1
Remote Port : 179 Local Port : 56008
State : Established Admin Status : Up
Conn. Established : 1 Conn. Dropped : 0
Passive : No Update-Source :
Cfg. Hold Time : 180 Cfg. Keep Alive : 60
Neg. Hold Time : 180 Neg. Keep Alive : 60
Up/Down Time : 00m:01w:03d Alt. Local-AS : 0
Local-AS Prepend : No
BFD : Disabled
Password :
Last Err Sent : No Error
Last SubErr Sent : No Error
Last Err Rcvd : No Error
Last SubErr Rcvd : No Error

Graceful-Restart : Enabled Gr. Restart Time : 120

```

Gr. Stalepath Time : 150
TTL                : 255
Weight             : 0
Remove Private-AS  : No
Local Cluster-ID   :
Fall-over          : No

Message statistics      Sent      Rcvd
-----
Open                   1         1
Notification           0         0
Updates                3         2
Keepalives            17995      18009
Route Refresh          0         0
Total                 17999      18012

Capability              Advertised      Received
-----
Route Refresh           Yes             Yes
Graceful Restart        Yes             Yes
Four Octet ASN          Yes             Yes
Address family IPv4 Unicast Yes             Yes
Address family IPv6 Unicast Yes             Yes
Address family L2VPN EVPN Yes             Yes

Address Family : L2VPN EVPN
-----

Rt. Reflect. Client : No
Allow-AS in         : 0
Max. Prefix         : 32768
NextHop-Self        :
Send Community      : extended
Advt. Interval      : 30
Soft Reconfig In    :
Default-Originate   :

Routemap In         :
Routemap Out        :

```

Showing information for BGP IPv4 unicast neighbors:

```

switch# show bgp ipv4 unicast neighbors
Codes: ^ Inherited from peer-group

VRF : default

BGP Neighbor 10.1.1.2 (Internal)
Description      :
Peer-group       :

Remote Router Id  : 10.1.1.2
Remote AS        : 1
Remote Port      : 0
State            : Idle
Conn. Established : 0
Passive          : No
Cfg. Hold Time   : 180
Neg. Hold Time   : 0
Up/Down Time     : 00h:00m:00s
Local-AS Prepend : No
BFD              : Disabled
Password         :
Last Err Sent    : No Error
Last SubErr Sent : No Error
Last Err Rcvd    : No Error
Last SubErr Rcvd : No Error

Local Router Id   : 1.0.0.1
Local AS          : 1
Local Port        : 0
Admin Status      : Up
Conn. Dropped     : 0
Update-Source     :
Cfg. Keep Alive   : 60
Neg. Keep Alive   : 0
Connect-Retry Time : 120
Alt. Local-AS     : 0
Slow Peer         : Yes

```



```

Graceful-Restart      : Enabled          Gr. Restart Time    : 120
Gr. Stalepath Time    : 150              Remove Private-AS   : No
TTL                   : 255              Local Cluster-ID    :
Weight                : 0                Fall-over           : No

Message statistics      Sent      Rcvd
-----
Open                   0          0
Notification           0          0
Updates                0          0
Keepalives             0          0
Route Refresh          0          0
Total                  0          0

Capability              Advertised   Received
-----
Route Refresh           Yes         No
Graceful Restart        Yes         No
Four Octet ASN          Yes         No
Add-Path                Yes         Yes
Address family IPv4 Unicast Yes         No
Address family IPv6 Unicast No          No
Address family L2VPN EVPN Yes          Yes

Address Family : IPv4 Unicast
-----

Rt. Reflect. Client : No                Send Community      :
Allow-AS in         : 0                  Advt. Interval      : 30
Max. Prefix         : 64000              Soft Reconfig In    :
Nexthop-Self        :                   Default-Originate    :
Update-Group        : 12

Routemap In         :
Routemap Out        :

ORF Type            : Prefix-list
ORF Capability       : Send

Cfg. Add-Path       : Send
Neg. Add-Path       : Send

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp paths

```
show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast | all}
    paths [vsx-peer]
show bgp l2vpn evpn paths
```

Description

Shows received BGP path information in the database.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family.

Examples

Showing received BGP path information from the specified IPv4 unicast neighbor:

```
switch# show bgp ipv4 unicast paths
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
VRF : default
Local Router-ID 9.0.0.1

   Network                Nexthop                PathID                Path
-----
*>e 9.0.0.0/24             9.0.0.2                0                    200 65534.65535 3.4 18.54934
3574.8570 5.6
*>e 100.0.0.0/24           9.0.0.2                0                    200
*>e 100.0.1.0/24           9.0.0.2                0                    200
*>e 100.0.2.0/24           9.0.0.2                0                    200
*>e 100.0.3.0/24           9.0.0.2                10                   200
*ae 100.0.3.0/24          9.0.0.3                5                    200
Total number of entries 6
```

Showing received BGP path information from the specified L2VPN EVPN neighbor:

```
switch# show bgp l2vpn evpn paths

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
```

```
VRF : default
Local Router-ID 9.0.0.2
```

Network	Nexthop	Path

Route Distinguisher: 10.1.1.54:32967 (L2VNI 30000)		
*> [2]:[0]:[0]:[00:06:f6:3f:e3:c1]:[]	1.1.1.20	100
*> [2]:[0]:[0]:[8c:60:4f:f2:f5:41]:[]	1.1.1.10	100
Total number of entries 2		



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp peer-group summary

```
show bgp [vrf <VRF-NAME>] {ipv4 unicast |  
    ipv6 unicast | all} peer-group <PEER-GROUP-NAME>  
    summary [vsx-peer]  
show bgp l2vpn evpn peer-group <PEER-GROUP-NAME> summary
```

Description

This command shows the peer-group information in the database.

Parameter	Description
vrf <VRF-NAME>	Shows the information for a specified VRF.
ipv4 unicast	Shows the information for an IPv4 unicast address family.
ipv6 unicast	Shows the information for an IPv6 unicast address family.
all	Shows the information for all address families and subaddress families.
<PEER-GROUP-NAME>	Shows the information for the BGP peer-group for the BGP instance.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not

Parameter	Description
	have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
l2vpn evpn	Shows the information for L2VPN EVPN address family. This parameter only applies to HPE Aruba Networking 8100, 8325, 9300/9300S, 8360 Switch series.

Examples

Showing the information from IPv4 unicast address families in `pg_name1` peer-group:

```
switch# show bgp ipv4 unicast peer-group pg_name1 summary
Codes: * Dynamic Neighbor
VRF : default
BGP Peer-Group Summary
=====
Local AS           : 1          BGP Router Identifier : 2.2.2.2
Peers              : 1          Dynamic Peer Count    : 3
Cfg. Hold Time     : 180       Cfg. Keep Alive       : 60

Neighbor          Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
10.0.0.1           1          8        10       00h:00m:58s   Established Up
*10.1.1.5          11         15       14       00h:10m:24s   Established Up
```

Showing the information from all address families in `pg_name1` peer-group:

```
switch# show bgp all unicast peer-group pg_name1 summary
Codes: * Dynamic Neighbor
VRF : default
BGP Peer-Group Summary
=====
Local AS           : 1          BGP Router Identifier : 2.2.2.2
Peers              : 1          Dynamic Peer Count    : 3
Cfg. Hold Time     : 180       Cfg. Keep Alive       : 60
Confederation Id   : 0

For address family: IPv4 Unicast
Neighbor          Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
10.0.0.1           1          8        10       00h:00m:58s   Established Up
*10.1.1.5          11         15       14       00h:10m:24s   Established Up

For address family: IPv6 Unicast
Neighbor          Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
1001::1002        11         12       12       00h:00m:07s   Established Up
2001::2002        11         12       12       00h:00m:07s   Established Up

For address family: L2VPN EVPN
Neighbor          Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
10.0.0.1           1          8        10       00h:00m:58s   Established Up
10.1.1.6           11         15       14       00h:10m:24s   Established Up
```

Showing the information from L2VPN EVPN address families in `pg_name1` peer-group:

```
switch# show bgp l2vpn evpn peer-group pg_name1 summary
VRF : default
BGP Peer-Group Summary
=====
```

```

Local AS          : 1          BGP Router Identifier : 2.2.2.2
Peers             : 1          Dynamic Peer Count   : 3
Cfg. Hold Time    : 180       Cfg. Keep Alive      : 60
Confederation Id  : 0

Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
10.0.0.1      1          8       10       00h:00m:58s   Established Up
*10.1.1.6     11         15      14       00h:10m:24s   Established Up

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp summary

```

show bgp [vrf <VRF-NAME>] {ipv4 unicast | ipv6 unicast | all}
    summary [vsx-peer]
show bgp l2vpn evpn summary

```

Description

This command shows a summary of the status of Border Gateway Protocol (BGP) connections.

Parameter	Description
ipv4 unicast	Selects to display the BGP summary information for the IPv4 subaddress family identifier.
ipv6 unicast	Selects to display the BGP summary information for the IPv6 subaddress family identifier.
all	Selects to display the BGP summary information for all VRFs and address-families.
vrf <VRF-NAME>	Selects to display information by VRFs by specifying the VRF name.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Parameter

Description

l2vpn evpn

Shows the information for L2VPN EVPN address family. This parameter only applies to HPE Aruba Networking 8100, 8325, 8360, 9300, 9300S Switch series

Examples

Showing BGP summary information for all address-families:

```
switch(config-bgp)# show bgp all summary
Codes: * Dynamic Neighbor
VRF : default
BGP Summary
  Local AS           : 100           BGP Router Identifier : 9.0.0.1
  Peers              : 1             Log Neighbor Changes  : No
  Cfg. Hold Time     : 180          Cfg. Keep Alive       : 60
  Confederation Id    : 0

Address-family : IPv4 Unicast
-----
Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
9.0.0.2        200         25       23       00h:17m:50s   Established Up
*10.1.1.5      11          26       24       00h:20m:26s   Established Up

Address-family : IPv6 Unicast
-----
Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
*2001::2002    11         3        3        00h:00m:14s   Established Up
9000::2        200        25       23       00h:17m:50s   Established Up

Address-family : VPNv4 Unicast
-----
Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
1.1.1.1        100        207      208      02h:54m:18s   Established Up
*3.3.3.4        11         26       24       00h:20m:26s   Established Up

Address-family : L2VPN EVPN
-----
Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
10.0.0.2       200        25       23       00h:17m:50s   Established Up
*10.1.1.6       11         26       24       00h:20m:26s   Established Up
VRF : v1
BGP Summary
  Local AS           : 100           BGP Router Identifier : 9.0.0.1
  Peers              : 1             Log Neighbor Changes  : No
  Cfg. Hold Time     : 180          Cfg. Keep Alive       : 60

Address-family : IPv4 Unicast
-----
Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
*4.4.4.4        11         26       24       00h:20m:26s   Established Up
9.0.0.2         200        25       23       00h:17m:50s   Established Up

Address-family : IPv6 Unicast
-----
Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
```

*3001::3002	11	3	3	00h:00m:14s	Established Up
9000::2	200	25	23	00h:17m:50s	Established Up

Showing BGP summary information for a specific VRF for IPv4 unicast network:

```
switch(config-bgp)# show bgp ipv4 unicast vrf v1 summary
Codes: * Dynamic Neighbor
VRF : v1
BGP Summary
  Local AS           : 100           BGP Router Identifier : 9.0.0.1
  Peers              : 1             Log Neighbor Changes  : No
  Cfg. Hold Time     : 180          Cfg. Keep Alive       : 60

Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
9.0.0.2       200        25       23       00h:17m:50s   Established Up
*10.1.1.5     11         26       24       00h:20m:26s   Established Up
```

Showing BGP summary information for L2VPN EVPN:

```
switch(config-bgp)# do show bgp l2vpn evpn summary
Codes: * Dynamic Neighbor
VRF : default
BGP Summary
  Local AS           : 100           BGP Router Identifier : 9.0.0.1
  Peers              : 1             Log Neighbor Changes  : No
  Cfg. Hold Time     : 180          Cfg. Keep Alive       : 60

Neighbor      Remote-AS  MsgRcvd  MsgSent  Up/Down Time  State      AdminStatus
10.0.0.2       200        25       23       00h:17m:50s   Established Up
10.1.1.6       11         26       24       00h:20m:26s   Established Up
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp l2vpn evpn

show bgp l2vpn evpn <ROUTE-TYPE>

Description

Shows the BGP L2VPN information.

Parameter	Description
<ROUTE-TYPE>	Specifies the routes filtered by NLRI route type. HPE Aruba Networking 6300, 6400, 8100, 8320, 8360, 9300, 9300S Switch series display information for route types 2-6.

Examples

Showing BGP L2VPN information for extcommunity:

```
switch# show bgp l2vpn evpn extcommunity
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 1 prefix: [1]:[ESI]:[EthTag]
EVPN Route-Type 2 prefix: [2]:{ESI}:{EthTag}:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 4 prefic: [4]:[ESI]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
EVPN Route-Type 6 prefix: [6]:[EthTag]:McastSrcIP]:[McastGrpIP]:[OrigIP]

VRF : default
Local Router-ID 2.2.2.2

Network                                     Nexthop
  Ext-Community
-----
Route Distinguisher: 2:2                    (L2VNI 1)
*>i [2]:[0]:[0]:[00:00:00:00:00:aa]:[100.100.1.2]  1.1.1.1
    1:1,100:100,00:00:00:00:00:11
*>i [3]:[0]:[1.1.1.1]                        1.1.1.1
    1:1

Route Distinguisher: 2:2                    (L2VNI 2)
*>i [2]:[0]:[0]:[00:00:00:00:00:aa]:[200.200.1.2]  3.3.3.3
    2:2,100:100,00:00:00:00:00:22
*>i [3]:[0]:[3.3.3.3]                        3.3.3.3
    2:2

Route Distinguisher: 1:1                    (L3VNI 10000)
*>i [2]:[0]:[0]:[00:00:00:00:00:aa]:[100.100.1.2]  1.1.1.1
    1:1,100:100,00:00:00:00:00:11

Route Distinguisher: 2:2                    (L3VNI 10000)
*>i [2]:[0]:[0]:[00:00:00:00:00:aa]:[200.200.1.2]  3.3.3.3
    2:2,100:100,00:00:00:00:00:22

Route Distinguisher: 4.4.4.4:40             (L2VNI 400)
*>i [3]:[0]:[4.4.4.4]                        4.4.4.4
    4:4,IGMP-MLD Proxy

Total number of entries 7
```

Showing BGP L2VPN information:


```

switch# show bgp l2vpn evpn 5.5.5.5:41-[6]:[0]:[30.1.36.30]:[232.0.0.8]:
VRF : default
BGP Local AS 65000          BGP Router-id 3.3.3.3

Network          : 5.5.5.5:41-[6]:[0]:[30.1.36.30]:[232.0.0.8]:[5.5.5.5]
Nexthop          : 5.5.5.5
vni              : 0                      vni_type       : L2VNI
Peer             : 2.2.2.2                Origin          : incomplete
Metric           : 0                      Local Pref      : 100
Weight           : 0                      Calc. Local Pref : 100
Best             : Yes                     Valid           : Yes
Type             : internal                Stale           : No
Originator ID    : 5.5.5.5
Aggregator ID    :
Aggregator AS    :
Atomic Aggregate :

AS-Path          :
Cluster List     : 2.2.2.2
Communities      :
Ext-Communities  : RT: 139:139

```

Showing BGP L2VPN information for route type 4:

```

switch# show bgp l2vpn evpn route-type 4

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 1 prefix: [1]:[ESI]:[EthTag]
EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 4 prefix: [4]:[ESI]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 16.16.16.16

Network          Nexthop  Metric  LocPrf  Weight
Path
-----
--
Route Distinguisher: 2.2.2.2:840          (L2VNI 0)
*>i [4]:[0000.0000.0001.0000.0001]:[2.2.2.2]  2.2.2.2  0      0      0      i
Route Distinguisher: 2.2.2.2:860          (L2VNI 0)
*>i [4]:[0000.0000.0001.0000.0002]:[2.2.2.2]  2.2.2.2  0      0      0      i
Route Distinguisher: 3.3.3.3:800          (L2VNI 0)
*>i [4]:[0000.0000.0001.0000.0001]:[3.3.3.3]  3.3.3.3  0      0      0      i
Route Distinguisher: 3.3.3.3:820          (L2VNI 0)
*>i [4]:[0000.0000.0001.0000.0003]:[3.3.3.3]  3.3.3.3  0      0      0      i
Total number of entries 4

```

Showing BGP L2VPN information for route type 6:

```

switch# show bgp l2vpn evpn route-type 6

Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```

EVPN Route-Type 6 prefix: [6]:[EthTag]:[McastSrcIP]:[McastGrpIP]:[OrigIP]

VRF: default
Router-ID not configured

Network                               Nexthop   Metric LocPrf  Weight
Path
-----
--
Route Distinguisher: 10.1.1.54:32967
*> [6]:[0]:[0.0.0.0]:[239.1.1.1]:[1.1.1.1] 1.1.1.1 0      100    32768  i
*> [6]:[0]:[10.1.1.30]:[225.1.1.1]:[1.1.1.1] 1.1.1.1 0      100    0      i
*> [6]:[0]:[10.1.1.40]:[225.1.1.2]:[1.1.1.1] 1.1.1.1 0      100    0      ?
*> [6]:[0]:[0.0.0.0]:[0.0.0.0]:[10.1.1.1] 10.1.1.1 0      100    0      i

Route Distinguisher: 2:2
*> [6]:[0]:[10.1.1.30]:[232.1.1.1]:[1.1.1.1] 1.1.1.1 0      100    0      ?
*> [6]:[0]:[10.1.1.40]:[239.1.1.1]:[2.2.2.2] 2.2.2.2 0      100    0      0
Total number of entries 5

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	Expanded route type range to include route type 7.
10.16	Expanded route type range to include route type 6.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp l2vpn evpn vni route-type

```
show bgp l2vpn evpn vni <VNI-Value> route-type <ROUTE-TYPE-Value>
```

Description

Shows the BGP L2VPN information for the particular EVPN VNI and routes type.

Parameter	Description
<VNI-Value>	Specifies the VNI.
<ROUTE-TYPE-Value>	Specifies the routes filtered by NLRI route type. HPE Aruba Networking 6300, 6400, 8100, 8320, 8360, 9300, 9300S Switch series display information for route types 2-6.

Examples

Showing BGP L2VPN information for the particular EVPN VNI and route type:

```
switch# show bgp l2vpn evpn vni 30000 route-type 5
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]

VRF : default
Router-ID not configured
Network                               Nexthop           Metric LocPrf
Weight Path
-----
Route Distinguisher: 1:100             (L3VNI 10000)
*>i [5]:[0]:[0]:[24]:[32.32.32.0]       3.3.3.3           0      100      0
?
*> [5]:[0]:[0]:[24]:[52.52.52.0]       1.1.1.1           0      100      0
?
*>i [5]:[0]:[0]:[64]:[aaa::]           3.3.3.3           0      100      0
?

Total number of entries 3
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.16	Expanded route type range to include route type 6.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp l2vpn evpn vtep

show bgp l2vpn evpn vtep <IP-address>

Description

Shows the BGP L2VPN information for the particular EVPN VTEP IP address.

Parameter	Description
<IP-address>	Specifies the VTEP IP address.

Examples

Showing BGP L2VPN information for the particular EVPN VTEP IP:

```
switch# show bgp l2vpn evpn vtep 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 2.2.2.2
```

Network		Nexthop	Metric
LocPrf	Weight	Path	

Route Distinguisher: 1.1.1.1:2 (L2VNI 2)			
*>i [2]:[0]:[0]:[00:00:00:00:00:33]:[10.1.1.10]		1.1.1.1	0
100	0	?	
*>i [2]:[0]:[0]:[00:00:00:00:00:33]:[1000::10]		1.1.1.1	0
100	0	?	
*>i [2]:[0]:[0]:[00:50:56:96:15:1c]:[10.1.1.1]		1.1.1.1	0
100	0	?	
*>i [2]:[0]:[0]:[00:50:56:96:15:1c]:[]		1.1.1.1	0
100	0	?	
*>i [3]:[0]:[1.1.1.1]		1.1.1.1	0
100	0	?	
Route Distinguisher: 1.1.1.1:2 (L3VNI 10000)			
*>i [2]:[0]:[0]:[00:00:00:00:00:33]:[10.1.1.10]		1.1.1.1	0
100	0	?	
*>i [2]:[0]:[0]:[00:00:00:00:00:33]:[1000::10]		1.1.1.1	0
100	0	?	
*>i [2]:[0]:[0]:[00:50:56:96:15:1c]:[10.1.1.1]		1.1.1.1	0
100	0	?	
*>i [2]:[0]:[0]:[00:50:56:96:15:1c]:[]		1.1.1.1	0
100	0	?	
Route Distinguisher: 1:100 (L3VNI 10000)			
*>i [5]:[0]:[0]:[24]:[10.1.1.0]		1.1.1.1	0
100	0	?	
*>i [5]:[0]:[0]:[64]:[1000::]		1.1.1.1	0
100	0	?	
Total number of entries 11			



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp l2vpn evpn vtep route-type

show bgp l2vpn evpn vtep <IP-address> route-type <ROUTE-TYPE-Value>

Description

Shows the BGP L2VPN information for the particular EVPN VTEP IP address and routes type.

Parameter	Description
<IP-address>	Specifies the VTEP IP address.
<ROUTE-TYPE-Value>	Specifies the routes filtered by NLRI route type. HPE Aruba Networking 6300, 6400, 8100, 8320, 8360, 9300, 9300S switches display information for route types 2, 3 and 5.

Examples

Showing BGP L2VPN information for the particular EVPN VTEP and route type:

```
switch# show bgp l2vpn evpn vtep 1.1.1.1 route-type 5
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]

VRF : default
Router-ID not configured

      Network
Metric LocPrf Weight Path
-----
Route Distinguisher: 1:100 (L3VNI 10000)
*>i [5]:[0]:[0]:[24]:[32.32.32.0] 1.1.1.1 0
   100 0 ?
*> [5]:[0]:[0]:[24]:[52.52.52.0] 1.1.1.1 0
   100 0 ?
*>i [5]:[0]:[0]:[64]:[aaa::] 1.1.1.1 0
   100 0 ?

Total number of entries 3
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp l2vpn evpn vtep vni

show bgp l2vpn evpn vtep <IP-address> vni <VNI-Value>

Description

Shows the BGP L2VPN information for the particular EVPN VTEP IP address and VNI.

Parameter	Description
<IP-address>	Specifies the VTEP IP address.
<VNI-Value>	Specifies the VNI.

Examples

Showing BGP L2VPN information for the particular EVPN VTEP IP and VNI:

```
switch# show bgp l2vpn evpn vtep 1.1.1.1 vni 10000
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 2.2.2.2

      Network                               Nexthop           Metric
      LocPrf   Weight   Path
-----
Route Distinguisher: 1.1.1.1:2              (L3VNI 10000)
*>i [2]:[0]:[0]:[00:00:00:00:00:33]:[10.1.1.10] 1.1.1.1           0
   100         0       ?
*>i [2]:[0]:[0]:[00:00:00:00:00:33]:[1000::10] 1.1.1.1           0
   100         0       ?
*>i [2]:[0]:[0]:[00:50:56:96:15:1c]:[10.1.1.1] 1.1.1.1           0
   100         0       ?
*>i [2]:[0]:[0]:[00:50:56:96:15:1c]:[] 1.1.1.1           0
   100         0       ?

Route Distinguisher: 1:100                  (L3VNI 10000)
*>i [5]:[0]:[0]:[24]:[10.1.1.0] 1.1.1.1           0
   100         0       ?
*>i [5]:[0]:[0]:[64]:[1000::] 1.1.1.1           0
   100         0       ?
Total number of entries 6
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp l2vpn evpn vtep vni route-type

show bgp l2vpn evpn vtep <VTEP-ID> vni <VNI-Value> route-type <ROUTE-TYPE-Value>

Description

Shows the BGP L2VPN information for the particular EVPN VTEP, VNI, and route type.

Parameter	Description
<VTEP-ID>	Specifies the VTEP.
<VNI-Value>	Specifies the VNI.
<ROUTE-TYPE-Value>	Specifies the route type. HPE Aruba Networking 6300, 6400, 8100, 8320, 8360, 9300/9300S Switch series display information for route types 2-5.

Examples

Showing BGP L2VPN information for the particular EVPN VTEP, VNI and route type 2:

```
switch# show bgp l2vpn evpn vtep 1.1.1.1 vni 10000 route-type 2
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 2.2.2.2

      Network                               Nexthop    Metric   LocPrf
Weight  Path
-----
Route Distinguisher: 1.1.1.1:2 (L3VNI 10000)
*>i [2]:[0]:[0]:[00:50:56:96:7d:03]:[10.1.1.1] 1.1.1.1    0        100      0
```

```

?
*>i [2]:[0]:[0]:[00:50:56:96:7d:03]:[]          1.1.1.1    0      100      0
?

Total number of entries 3

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show bgp ip unicast

show bgp ip unicast [<A.B.C.D/M> | protected]

Description

This command shows configuration for all BGP routes. Protected Routes will have two Nexthops and the backup path is identified with the status code 'b'

Usage

- Protected Routes will have two Nexthops
- The backup path is identified with the status code 'b'

Examples

Showing BGP IP routes:

```

switch# show bgp ip unicast
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, e external S Stale, R Removed, a additional-paths,
               b backup path
Origin codes: i - IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 200.0.0.1

Network      Nexthop      Metric      LocPrf      Weight
  Path
Route Distinguisher: 1:0
*> 10.10.10.0/24      0.0.0.0      0           100         0
  ?

```



```

* i 10.10.10.0/24          10.10.10.1      0          100          0
?
*>i 20.20.20.0/24         10.10.10.1      0          100          0
?
*=i 20.20.20.0/24         20.20.20.2      0          100          0
?
*=i 20.20.20.0/24         40.40.40.2      0          100          0
?
*> 30.30.30.0/24          0.0.0.0         0          100          0
?
* i 30.30.30.0/24         30.30.30.1      0          100          0
?
*=i 40.40.40.0/24         20.20.20.2      0          100          0
?
*>i 40.40.40.0/24         30.30.30.1      0          100          0
?
*=i 40.40.40.0/24         40.40.40.2      0          100          0
?
*> 200.0.0.0/24           0.0.0.0         0          100          0
i
*>i 201.0.0.0/24          20.20.20.2      0          100          0
i
*bi 201.0.0.0/24          40.40.40.2      0          100          0
i
Total number of entries 13
```

```

Showing protected BGP IP routes:

```

switch# show bgp ip unicast protected
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
 i internal, e external S Stale, R Removed, a additional-paths,
 b backup path
Origin codes: i - IGP, e - EGP, ? - incomplete

VRF : default
Local Router-ID 200.0.0.1

Network Nexthop Metric LocPrf Weight
 Path
Route Distinguisher: 1:0
*>i 201.0.0.0/24 20.20.20.2 0 100 0
i
*bi 201.0.0.0/24 40.40.40.2 0 100 0
i
Total number of entries 2

```

Showing BGP routes for a specific IP address:

```

switch# show bgp ip unicast 201.0.0.0/24
VRF : default
BGP Local AS 1 BGP Router-id 200.0.0.1

Network : 201.0.0.0/24 Nexthop : 20.20.20.2
Peer : 10.10.10.1 Origin : IGP
Metric : 0 Local Pref : 100
Weight : 0 Calc. Local Pref : 100

```

```

Best : Yes Valid : Yes
Type : internal Stale : No
Originator ID : 201.0.0.1
Aggregator ID :
Aggregator AS :
Atomic Aggregate :
RFD Flaps : 0 RFD Penalty : 0
AS-Path :
Cluster List : 10.10.10.1
Communities :
Ext-Communities :
Backup : No
Network : 201.0.0.0/24 Nexthop : 40.40.40.2
Peer : 30.30.30.1 Origin : IGP
Metric : 0 Local Pref : 100
Weight : 0 Calc. Local Pref : 100
Best : No Valid : Yes
Type : internal Stale : No
Originator ID : 201.0.0.1
Aggregator ID :
Aggregator AS :
Atomic Aggregate :
RFD Flaps : 0 RFD Penalty : 0
AS-Path :
Cluster List : 30.30.30.1
Communities :
Ext-Communities :
Backup : Yes
` ``

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release    | Modification                            |
|------------|-----------------------------------------|
| 10.15      | Introduces the <b>protected</b> option. |
| 10.14.1000 | Command introduced.                     |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip ospf routes

```

show ip ospf [<PROCESS-ID>] routes
 [<IPV4-ADDR>/<MASK>] protected [all-vrfs | vrf <VRF-NAME>]

```

## Description

Displays OSPF routing information.

| Parameter      | Description                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| <IPv4-ADDR>    | Specify an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.                     |
| <MASK>         | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 32. |
| <PROCESS-ID>   | Enter an OSPF process ID to display OSPF neighbor information for the particular OSPF process. Range: 1 to 65535.              |
| all-vrfs       | Select to display neighbor information for all VRFs.                                                                           |
| vrf <VRF-NAME> | Specify the name of a VRF. Default: default.                                                                                   |
| protected      | Selects a protected route. Specifying an IPv4 address will select protected route for that prefix.                             |

## Examples

Showing OSPF routing table information:

```
switch# show ip ospf routes
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table

Total Number of Routes : 2

10.1.1.0/24 (i) area: 0.0.0.0
 directly attached to interface 1/1/1, cost 1 distance 110
20.1.1.0/24 (I)
 via 10.1.1.2 interface 1/1/1, cost 2 distance 110
```

Showing OSPF routing table information for a specific subnet:

```
switch# show ip ospf routes 10.1.1.0/2
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table for prefixes 10.1.1.0/24

Total Number of Routes : 1

10.1.1.0/24 (i) area: 0.0.0.0
 directly attached to interface 1/1/1, cost 1 distance 110
```

Showing OSPF routing table information for a specific protected subnet on the default VRF:

```
switch# show ip ospf routes 211.0.0.0/24 protected vrf default
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes for prefixes 211.0.0.0/24
```

```

211.0.0.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 122
 bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 1

```

Showing OSPF routing table information for a specific protected subnet on all VRFs

```

switch# show ip ospf routes 211.0.0.0/24 protected all-vrfs
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes for prefixes 211.0.0.0/24

211.0.0.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 122
 bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 1

```

Showing OSPF routing table information for a specific protected subnet:

```

switch# show ip ospf routes 211.0.0.0/24 protected
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes for prefixes 211.0.0.0/24

211.0.0.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 122
 bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 1

```

Showing OSPF routing table information for all protected routes:

```

switch# show ip ospf routes 211.0.0.0/24 protected
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes

120.120.120.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 120
 bkp 130.130.130.1, interface vlan22, cost 230

140.140.140.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 130
 bkp 130.130.130.1, interface vlan22, cost 220

```

```

211.0.0.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 122
 bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 3

OSPFs Process ID 1, VRF red, Protected Routes

Total Number of Protected Routes: 0

```

Showing OSPF routing table information for protected routes on the default VRF:

```

switch# show ip ospf routes protected vrf default
Codes: i - Intra-area route, I - Inter-area route
 E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes

140.140.140.0/24 (i) area: 0.0.0.0
 via 130.130.130.1, interface vlan22, cost 130
 bkp 110.110.110.1, interface vlan20, cost 220

211.0.0.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 122
 bkp 130.130.130.1, interface vlan22, cost 132

120.120.120.0/24 (i) area: 0.0.0.0
 via 110.110.110.1, interface vlan20, cost 120
 bkp 130.130.130.1, interface vlan22, cost 230

Total Number of Routes : 3

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                                              |
|------------------|-----------------------------------------------------------|
| 10.15            | Introduces the <b>protected</b> parameter.                |
| 10.14            | Supported process ID range expanded from 1-63 to 1-65535. |
| 10.07 or earlier | --                                                        |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show running-config bgp

show running-config bgp [vsx-peer]

## Description

This command shows all configured BGP commands.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

EVPN only applies to HPE Aruba Networking 8100, 8325, 8360, 9300/9300S, 6300, 6400 Switch series.

```
switch# show running-config bgp
router bgp 65534.65535
 bgp asnotation dotted
 network 2.2.2.0/24
 neighbor 1.1.1.2 remote-as 65533.65535
 address-family ipv4 unicast
 neighbor 1.1.1.2 activate
 neighbor 1.1.1.2 route-map A out
 vrf v1
 address-family l2vpn evpn
 neighbor 1.1.1.2 activate
 neighbor 1.1.1.2 send-community extended
 exit-address-family
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# timers bgp

timers bgp <KEEPALIVE> <HOLDTIME>  
no timers bgp <KEEPALIVE> <HOLDTIME>

## Description

The command adjusts BGP network timers.

The **no** form of this command resets the BGP timers to defaults of 60 seconds for the keepalive timer and 180 seconds for the holdtime timer.

| Parameter                      | Description                                                              |
|--------------------------------|--------------------------------------------------------------------------|
| <code>&lt;KEEPALIVE&gt;</code> | Sets the value for keepalive timer. Default: 60 seconds. Range: 0-65535. |
| <code>&lt;HOLDTIME&gt;</code>  | Sets the value for holdtime timer. Default: 180 seconds. Range: 0-65535. |

## Usage

- The keepalive timer is the number of seconds a BGP peer waits for a keep-alive message from a BGP peer before deciding the connection is down.

The holdtime timer is the number of seconds a BGP peer waits after not receiving a keepalive, update, or notification message before declaring that a connection with BGP peer is down.

- When a session is started, BGP negotiates holdtime with the neighbor, and selects the smaller value. The keepalive timer is then set based on the negotiated holdtime and the configured keepalive time.

## Examples

```
switch(config-bgp)# timers bgp 100 150
switch(config-bgp)# no timers bgp
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-bgp      | Administrators or local user group members with execution rights for this command. |

## vrf

```
vrf <VRF-NAME>
no vrf <VRF-NAME>
```

## Description

Creates a VRF instance named `<VRF-NAME>` and then enters its context. Use **default** for `<VRF-NAME>` to enter the default VRF configure context.

Except for the default VRF, the **no** form of the command deletes the named VRF instance and any IP configuration for interfaces or SVI linked to default VRF. The default VRF cannot be deleted and a warning is given if attempted. To erase the Route-Distinguisher and Route-Targets, enter the default VRF context and delete them manually one by one.

| Parameter                     | Description                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------|
| <code>&lt;VRF-NAME&gt;</code> | Specifies the VRF name. Range: Up to 32 alphanumeric characters. The <b>mgmt</b> VRF cannot be used. |

## Examples

Creating the VRF named **cust\_A** and then entering its context:

```
switch(config)# vrf cust_A
```

Entering the **default** VRF context:

```
switch(config)# vrf default
```

Deleting the VRF named **test**:

```
switch(config)# no vrf test
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                   |
|------------------|--------------------------------|
| 10.09            | Added default VRF information. |
| 10.07 or earlier | --                             |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# BIDIR-PIM commands

## ip pim-bidir

```
ip pim-bidir [enable | disable]
```

### Description



Enables or disables PIM-Bidir in the designated interface. This command works in the interface context, including loopback. The IP address must be configured on the interface to enable BIDIR-PIM.

| Parameter | Description                                  |
|-----------|----------------------------------------------|
| [enable]  | Enables PIM Bidirectional on the interface.  |
| [disable] | Disables PIM Bidirectional on the interface. |

## Example

Enabling PIM-Bidir:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-bidir enable
```

Disabling PIM-Bidir:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-bidir disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ip pim-bidir hello-delay

```
ip pim-bidir hello-delay <DELAY-VALUE>
no ip pim-bidir hello-delay <DELAY-VALUE>
```

### Description

Changes the maximum time, in seconds, before the router transmits the initial PIM hello message on the current interface. The **no** form of this command removes the currently configured value and sets it to default. The default value is 5.

| Parameter                        | Description                                                     |
|----------------------------------|-----------------------------------------------------------------|
| <code>&lt;DELAY-VALUE&gt;</code> | Configures the given value as the hello interval. Range: <0-5>. |

## Usage

In cases where a new L3 interface activates with connections to multiple routers, if all of the connected routers sent hello packets at the same time, the receiving router could momentarily become overloaded. This value randomizes the transmission delay to a time between 0 and the hello delay setting. Using 0 means no delay. After the router sends the initial hello packet to a newly detected L3 interface, it sends subsequent hello packets according to the current Hello Interval setting.

## Example

Changing the maximum time before the router transmits the initial PIM hello message on the current interface to 4 seconds:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-bidir hello-delay 4
```

Removing the maximum time before the router transmits the initial PIM hello message on the current interface from 4 seconds and reverting to the default:

Disabling hello-delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ip pim-bidir hello-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ip pim-bidir lan-prune-delay

```
ip pim-bidir lan-prune-delay
no ip pim-bidir lan-prune-delay
```

## Description

Enables the LAN prune delay option on the current interface. The **no** form of this command disables the LAN prune delay option.

## Usage

With LAN prune delay enabled, the router informs the downstream neighbors how long it waits before pruning a flow after receiving a prune request. Other downstream routers on the same subnet must send a join to override the prune before the LAN prune delay time for the flow to continue. This prompts any downstream neighbors with multicast receivers that continue to belong to the flow to reply with a join. If no joins are received after the LAN prune delay and override-interval period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN prune delay setting. It is enabled by default.

## Example

Enabling the LAN prune delay option:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-bidir lan-prune-delay
```

Disabling the LAN prune delay option:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ip pim-bidir lan-prune-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ip pim-bidir override-interval

```
ip pim-bidir override-interval <INTERVAL-VALUE>
no ip pim-bidir override-interval <INTERVAL-VALUE>
```

## Description

Configures the override interval that gets inserted into the Override Interval field of a LAN prune delay option. The no form of this command removes the currently configured value and sets it to the default. The default value is 2500 milliseconds.

| Parameter                           | Description                                                              |
|-------------------------------------|--------------------------------------------------------------------------|
| <code>&lt;INTERVAL-VALUE&gt;</code> | Specifies override interval value.<br>Range: 500-6000.<br>Default: 2500. |

## Example

Configuring the override interval value to 4000:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-bidir override-interval 4000
```

Removing the override interval value and setting to default:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ip pim-bidir override-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# ip pim-bidir propagation-delay

```
ip pim-bidir propagation-delay <DELAY-VALUE>
no ip pim-bidir propagation-delay <DELAY-VALUE>
```

## Description

Configures the propagation delay that gets inserted into the propagation delay field of a LAN prune delay option. The **no** form of this command removes any configuration and resets to the default. Default: 500 milliseconds.

| Parameter                        | Description                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------|
| <code>&lt;DELAY-VALUE&gt;</code> | Specifies the propagation delay in milliseconds.<br>Range: 250-2000.<br>Default: 500. |

## Example

Configuring the propagation delay to 400 milliseconds:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-bidir propagation-delay 400
```

Removing the propagation delay and setting to default:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ip pim-bidir propagation-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## no ip pim-bidir

```
no ip pim-bidir
```

### Description

Removes all PIM-Bidir configurations for the interface.

### Example

Removing PIM-Bidir configurations for the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ip pim-bidir
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip pim dfe

```
show ip pim dfe [vrf <VRF-NAME> | all-vrfs]
```

### Description

Displays the Designated Forwarder information for a given interface and RP address in the topology. This prints the winner address along with winner metric details to reach RPA and its uptime details for a given VRF. If a VRF is not specified, the default is displayed.

| Parameter  | Description         |
|------------|---------------------|
| <VRF-NAME> | Specifies the VRF.  |
| [all-vrfs] | Specifies all VRFs. |

### Example

Displaying the Designated Forwarder information for the default VRF:

```
switch# show ip pim dfe
PIM BIDIR DFE Information

VRF : default
Total number of DFE entries : 2

Interface RPA DF Winner Metric Uptime
(HH:MM:SS)

vlan10 1.1.1.1 10.1.1.3 100 00:33:15
vlan30 1.1.1.1 30.1.1.1 0 00:33:16
```

Displaying the Designated Forwarder information for VRF red:

```
switch# show ip pim dfe vrf red
PIM BIDIR DFE Information

VRF : red
Total number of DFE entries : 1

Interface RPA DF Winner Metric Uptime
(HH:MM:SS)

vlan50 5.5.5.5 50.1.1.5 200 00:34:42
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ip pim dfe

```
show ip pim dfe <INTERFACE-NAME> <RP-ADDRESS>
```

## Description

Displays the Designated Forwarder information for all interfaces of an RP address in the topology. This prints the winner address along with winner metric details to reach RPA and its uptime details for a given VRF. If a VRF is not specified, the default is displayed.

| Parameter        | Description               |
|------------------|---------------------------|
| <INTERFACE-NAME> | Specifies the interface.  |
| <RP-ADDRESS>     | Specifies the RP address. |

## Example

Displaying the Designated Forwarder information for 1.1.1.1:

```
switch# show ip pim dfe vlan10 1.1.1.1
PIM BIDIR DFE Information
```

```
VRF : default
```

| Interface<br>(HH:MM:SS) | RPA     | DF Winner | Metric | Uptime   |
|-------------------------|---------|-----------|--------|----------|
| -----                   | -----   | -----     | -----  | -----    |
| -----                   |         |           |        |          |
| vlan10                  | 1.1.1.1 | 10.1.1.3  | 100    | 00:33:15 |



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show running-config pim

show running-config pim

### Description

Displays the current running configuration in the router pim context.

### Example

Displaying the current running configuration in the router pim context:

```
switch# show running-config pim
router pim
 enable
 rp-address 10.0.0.4
 rp-candidate source-ip-interface loopback1 group-prefix 239.1.1.1/32
 multicast-route-limit 1024
 active-active
 anycast-rp source-directly-connected
router pim vrf green
 enable
 rp-address 30.0.0.4
 rp candidate source-ip-interface loopback1 group-prefix 224.0.0.0/4
 multicast-route-limit 1024
 active-active
 anycast-rp source-directly-connected
interface loopback11
 ip pim-bidir enable
interface loopback44
 ip pim-bidir enable
interface vlan30
 ip pim-bidir enable
interface vlan500
 ip pim-bidir enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification          |
|---------|-----------------------|
| 10.13   | BIDIR PIM introduced. |



## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## BIDIR-PIM6 commands for IPv6

### ipv6 pim6-bidir

ipv6 pim6-bidir [enable | disable]

#### Description

Enables or disables PIM-Bidir in the designated interface. This command works in the interface context, including loopback. The IP address must be configured on the interface to enable BIDIR-PIM.

| Parameter | Description                                   |
|-----------|-----------------------------------------------|
| enable    | Enables PIM6 Bidirectional on the interface.  |
| disable   | Disables PIM6 Bidirectional on the interface. |

#### Example

Enabling PIM-Bidir:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 2001:db8::1/64
switch(config-if-vlan)# ipv6 pim6-bidir enable
```

Disabling PIM-Bidir:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 2001:db8::1/64
switch(config-if-vlan)# ipv6 pim6-bidir disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ipv6 pim6-bidir hello-interval

```
ipv6 pim6-bidir hello-interval <interval-value>
no ipv6 pim6-bidir hello-interval <interval-value>
```

### Description

Changes the frequency at which the router transmits PIM hello messages on the current subnet. The router uses hello packets to inform neighbor routers of its presence and to compute the hello hold time. Hello hold time informs neighbor routers estimated wait time for the next hello packet from the router. Shortening the hello interval reduces the hello hold time. Default is set to 30 seconds.

The **no** form of this command disables the frequency of PIM hello messages on the current subnet.

| Parameter      | Description                                  |
|----------------|----------------------------------------------|
| interval-value | Configures the given value as hello interval |

### Example

Configuring hello- interval on interface 1/1/4:

```
switch(config)# interface 1/1/4
switch(config-if)# ipv6 pim6-bidir hello-interval 60
switch(config-if)#
```

Disabling hello-interval:

```
switch(config-if)# no ipv6 pim6-bidir hello-interval 60
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

### Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# ipv6 pim6-bidir hello-delay

```
ipv6 pim6-bidir hello-delay <delay-value>
no ipv6 pim6-bidir hello-delay <delay-value>
```

## Description

Changes the maximum time, in seconds, before the router transmits the initial PIM hello message on the current interface. The default is set to 5.

The **no** form of this command disables the delay of PIM hello messages on the current subnet.

| Parameter   | Description                                  |
|-------------|----------------------------------------------|
| delay-value | Configures the given value as hello interval |

## Example

Configuring hello-delay on a interface vlan40:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-bidir hello-delay 4
```

Disabling hello-delay:

```
switch(config-if-vlan)# no ipv6 pim6-bidir hello-delay 4
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# ipv6 pim6-bidir lan-prune-delay

```
ipv6 pim6-bidir lan-prune-delay
no ipv6 pim6-bidir lan-prune-delay
```

## Description

Enables the LAN prune delay option on the current interface. With lan-prune-delay enabled, the router informs downstream neighbors on the wait time before pruning a flow after receiving a prune request.

The **no** form of this command removes the default setting.

## Example

Configuring lan-prune-delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-bidir lan-prune-delay
```

Disabling lan-prune-delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-bidir lan-prune-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ipv6 pim6-bidir override-interval

```
ipv6 pim6-bidir override-interval <interval-value>
no ipv6 pim6-bidir override-interval <interval-value>
```

### Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option. The default is set to 2500 milliseconds.

The **no** form of this command removes the configured value and sets it to default.

| Parameter      | Description                                     |
|----------------|-------------------------------------------------|
| interval-value | Configures the given value as override interval |

## Example

Configuring override-interval:

```
switch(config)# interface vlan40
```

```
switch(config-if-vlan) # ipv6 pim6-bidir override-interval 4000
```

### Disabling override-interval

```
switch(config-if-vlan) # no ipv6 pim6-bidir override-interval 4000
switch(config-if-vlan) # no ipv6 pim6-bidir override-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ipv6 pim6-bidir propagation-delay

```
ipv6 pim6-bidir propagation-delay <delay-value>
no ipv6 pim6-bidir propagation-delay <delay-value>
```

### Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option. The default is set to 500 milliseconds.

The **no** form of this command removes the configured value and sets it to default.

| Parameter   | Description                                     |
|-------------|-------------------------------------------------|
| delay-value | Configures the given value as propagation delay |

### Example

Enabling propagation-delay:

```
switch(config) # interface vlan40
switch(config-if-vlan) # ipv6 pim6-bidir propagation-delay 400
```

Disabling propagation-delay:

```
switch(config-if-vlan)# no ipv6 pim6-bidir propagation-delay 400
switch(config-if-vlan)# no ipv6 pim6-bidir propagation-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ipv6 pim6 dfe

```
show ipv6 pim6 dfe [vrf <vrf-name> | all-vrfs] <interface-name> <rp-address>
```

## Description

Displays the Designated Forwarder information for a given interface of a rp-address in the topology.

| Parameter      | Description                                        |
|----------------|----------------------------------------------------|
| dfe            | Displays PIM DFE information                       |
| vrf            | Displays DFE details for a specific VRF            |
| vrf-name       | Displays details for the given VRF name            |
| all-vrfs       | Displays DFE information for all VRFs              |
| interface-name | Displays PIM DFE Information for a given interface |
| rp-address     | Displays PIM DFE information on an RPA             |

## Example

Displaying PIM DFE information:

```
Switch# show ipv6 pim6 dfe
PIM BIDIR DFE Information
VRF : default
Total number of DFE entries : 2
Interface RPA DF Winner Metric Uptime (HH:MM:SS)

vlan10 2001:db8::1 fe80::1 100 00:33:15
```

|        |             |         |   |          |
|--------|-------------|---------|---|----------|
| vlan30 | 2001:db8::1 | fe80::2 | 0 | 00:33:16 |
|--------|-------------|---------|---|----------|

Displaying PIM DFE information for a specific VRF:

```
Switch# show ipv6 pim6 dfe vrf red
PIM BIDIR DFE Information
VRF : red
Total number of DFE entries : 1
Interface RPA DF Winner Metric Uptime (HH:MM:SS)

vlan50 2001:db8:5::5 fe80::3 200 00:34:42
```

Displaying PIM DFE information for a given interface:

```
Switch# show ipv6 pim6 dfe vlan10 2001:db8::1
PIM BIDIR DFE Information
VRF : default
Interface RPA DF Winner Metric Uptime (HH:MM:SS)

vlan10 2001:db8::1 fe80::1 100 00:33:15
```

Displaying PIM DFE information for an RPA:

```
Switch# show ipv6 pim6 dfe vlan100 2001:db8::1
PIM BIDIR DFE Information
VRF : default
Interface RPA DF Winner Metric Uptime (HH:MM:SS)

vlan10 2001:db8::1 fe80::1 NA 00:33:15
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

### boot set-default

```
boot set-default {primary | secondary}
```

#### Description

Sets the default operating system image to use when the system is booted. Changes to this setting may impact other features, such as the job scheduler feature configured via the **reload at** or **reload after** commands.

| Parameter | Description                                           |
|-----------|-------------------------------------------------------|
| primary   | Selects the primary network operating system image.   |
| secondary | Selects the secondary network operating system image. |

#### Example

Selecting the primary image as the default boot image:

```
switch# boot set-default primary
Default boot image set to primary.
```



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

#### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

#### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### boot system

```
boot system [primary | secondary | serviceos]
```



## Description

Reboots all modules on the switch. By default, the configured default operating system image is used. Optional parameters enable you to specify which system image to use for the reboot operation and for future reboot operations.

| Parameter              | Description                                                                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>primary</code>   | Selects the primary operating system image for this reboot and sets the configured default operating system image to <b>primary</b> for future reboots.                                                                                                                                                     |
| <code>secondary</code> | Selects the secondary operating system image for this reboot and sets the configured default operating system image to <b>secondary</b> for future reboots.                                                                                                                                                 |
| <code>serviceos</code> | Selects the service operating system for this reboot. Does not change the configured default operating system image. The service operating system acts as a standalone bootloader and recovery OS for switches running the AOS-CX operating system and is used in rare cases when troubleshooting a switch. |

## Usage

This command reboots the entire system. If you do not select one of the optional parameters, the system reboots from the configured default boot image.

You can use the **show images** command to show information about the primary and secondary system images.

Choosing one of the optional parameters affects the setting for the default boot image:

- If you select the **primary** or **secondary** optional parameter, that image becomes the configured default boot image for future system reboots. The command fails if the switch is not able to set the operating system image to the image you selected.

You can use the **boot set-default** command to change the configured default operating system image.

- If you select **serviceos** as the optional parameter, the configured default boot image remains the same, and the system reboots all management modules with the service operating system.

If the configuration of the switch has changed since the last reboot, when you execute the **boot system** command you are prompted to save the configuration and you are prompted to confirm the reboot operation.

Saving the configuration is not required. However, if you attempt to save the configuration and there is an error during the save operation, the **boot system** command is aborted.

## Examples

Rebooting the system from the configured default operating system image:

```
switch# boot system
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.
```

```
The system is going down for reboot.
```

Rebooting the system from the secondary operating system image, setting the secondary operating system image as the configured default boot image:

```
switch# boot system secondary
Default boot image set to secondary.

Do you want to save the current configuration (y/n)? n

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.
```

Canceling a system reboot:

```
switch# boot system

Do you want to save the current configuration (y/n)? n

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? n
Reboot aborted.
switch#
```



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show boot-history

```
show boot-history [all|{vsf member <1-10>}]
```

### Description

Shows boot history information. When no parameters are specified, shows the most recent information about the current boot operation, and the three previous boot operations for the switch. When the **all**

parameter is specified, the output of this command shows the boot information for the active management module.



---

To view boot-history on a standby, the command must be sent on the conductor console.

---

| Parameter                            | Description                                                        |
|--------------------------------------|--------------------------------------------------------------------|
| <code>all</code>                     | Optional. Shows boot information for the active management module. |
| <code>vsf member &lt;1-10&gt;</code> | Optional. Display boot history for the specified VSF member        |

## Usage

This command displays the boot-index, boot-ID, and up time in seconds for the current boot. If there is a previous boot, it displays boot-index, boot-ID, reboot time (based on the time zone configured in the system) and reboot reasons. Previous boot information is displayed in reverse chronological order.

The output of this command includes the following information:

| Parameter                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index                       | The position of the boot in the history file. Range: 0 to 3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Boot ID                     | A unique ID for the boot . A system-generated 128-bit string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Current Boot, up for <time> | For the current boot, the <b>show boot-history</b> command shows the number of seconds the module has been running on the current software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <Timestamp>: boot reason    | <p>For previous boot operations, the <b>show boot-history</b> command shows the time at which the operation occurred and the reason for the boot. The reason for the boot is one of the following values:</p> <ul style="list-style-type: none"><li>▪ <b>&lt;DAEMON-NAME&gt; crash:</b> The daemon identified by &lt;DAEMON-NAME&gt; caused the module to boot.</li><li>▪ <b>Kernel crash:</b> The operating system software associated with the module caused the module to boot.</li><li>▪ <b>Uncontrolled reboot:</b> The reason for the reboot is not known.</li><li>▪ <b>Reboot requested through database:</b> The reboot occurred because of a request made through the CLI or other API.</li></ul> |

## Examples

Showing the boot history of the active management module:

```

switch# show boot-history
Management module
=====

Index : 2
Boot ID : c34a2c2499004a02bbeeff4992e1fdbd
Current Boot, up for 1 days 13 hrs 13 mins 27 secs

Index : 1
Boot ID : bfba9bc486304e57904ac717a0ccbdcd
02 Sep 23 02:55:33 : CPU request reset with 0x20201, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:55:33 : Switch boot count is 2

Index : 0
Boot ID : a88a71b7ca9a4574af7e3b811ddfdc7e
02 Sep 23 02:49:26 : Reboot requested by user, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:50:02 : Switch boot count is 1

Index : 3
Boot ID : f00ba10c8c44457f83fee303d014a89a
25 Aug 23 10:27:42 : Power on reset with 0x1, Version: FL.10.14.0000-1465-
g9df95249d06b0~dirty
25 Aug 23 10:28:18 : Switch boot count is 3
25 Aug 23 10:29:02 : Primary overtemperature fault detected with 0x2 in PSU 1/1

```

Showing the boot history of the active management module and all line modules:



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## Breakout cable support commands

## split

```
split [<COUNT>] [<SPEED>] [confirm]
no split [confirm]
```

### Description

Splits a port into multiple interfaces. Only ports capable of supporting breakout cables or SR4/eSR4/eDR4 optics can be split.

| Parameter | Description                                                                               |
|-----------|-------------------------------------------------------------------------------------------|
| <COUNT>   | Specifies the number of child interfaces to activate upon splitting the port. Default: 4. |
| <SPEED>   | Specifies the speed for the child interfaces.                                             |
| confirm   | Specifies the confirmation of port splitting.                                             |

### Usage

- Some switch interfaces support different split counts depending on the installed transceiver. For these interfaces, the number of child interfaces to activate can be specified. If omitted, the default is 4. For transceivers capable of supporting multiple split modes, the closest mode with enough lanes is used.
- Some transceivers also support multiple split modes with different speeds. For example, 2x200G or 2x100G. When a speed is not specified, the highest available speed for the split count is used. To select a different split mode with a lower speed, the desired speed must be specified.



When the current transceiver does not support the configured split speed, the interface will remain down with an `Invalid speed` error.



Ports that are not splittable in the currently applied interface profile can be configured as split, but remain in a **down** state until a compatible profile is selected and the switch rebooted to apply it.

The splittable ports for all models are shown in the table below:

| Model                                                                              | Description                                         | Port info                                                      |
|------------------------------------------------------------------------------------|-----------------------------------------------------|----------------------------------------------------------------|
| <b>9300 Switch Series</b> <ul style="list-style-type: none"> <li>R8Z96A</li> </ul> | 9300-32D 32p 100/200/400G QSFP-DD p 10G SFP+ Switch | Porte 1-32 are splittable.<br>400G SR8 can split two, four, or |

| Model                                                                                                   | Description                                                                                                 | Port info                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                         |                                                                                                             | <p>eight ways (8-way splitting available on the 9300-32D only).</p> <p>Some ports are splittable depending on the interface profile use. See the <a href="#">Installation and Getting Started Guide</a> for more information.</p>                                                                                                                                                                                                                      |
| <b>9300S Switch Series</b> <ul style="list-style-type: none"> <li>▪ S0F95A</li> <li>▪ S0F96A</li> </ul> | <p>9300S 32P QSFP28 100G 8p QSFP-DD 400G TAA Switch</p> <p>9300S 32P QSFP28 100G 8p QSFP-DD 400G Switch</p> | <p>9-12, 17-24, and 29-32 ports are splittable.</p> <p>400G SR8 can split two or four ways</p> <p>QSFP-DD ports are capable of operating at:</p> <ul style="list-style-type: none"> <li>▪ 100G ports</li> <li>▪ 40G ports</li> <li>▪ Split into 4 individual 25G or 10G ports</li> </ul> <p>Some ports are splittable depending on the interface profile use. See the <a href="#">Installation and Getting Started Guide</a> for more information.</p> |

## Examples

Splitting an interface two ways on a 9300 Series Switch using the default for speed, taking the port capability (400G), and assuming 200G:

```
switch(config)# interface 1/1/1
switch(config-if)# split 2
This command will disable the specified port, clear its configuration,
and split it into multiple interfaces.

Continue (y/n)? y

switch(config-if)# show interface brief
```

| Port    | Native VLAN | Mode   | Type     | Enabled | Status | Reason | Speed (Mb/s) | Description |
|---------|-------------|--------|----------|---------|--------|--------|--------------|-------------|
| 1/1/1:1 | --          | routed | 400G-SR8 | yes     | up     |        | 200000       |             |
| 1/1/1:2 | --          | routed | 400G-SR8 | yes     | up     |        | 200000       |             |

Changing the interface to 2x100G mode:

```
switch(config)# interface 1/1/1
switch(config-if)# split 2 100g
This command will clear the configuration for all split interfaces of
this port.
```

Continue (y/n)? **y**

switch(config-if) # **show interface brief**

| Port    | Native VLAN | Mode   | Type     | Enabled | Status | Reason | Speed (Mb/s) | Description |
|---------|-------------|--------|----------|---------|--------|--------|--------------|-------------|
| 1/1/1:1 | --          | routed | 400G-SR8 | yes     | up     |        | 100000       |             |
| 1/1/1:2 | --          | routed | 400G-SR8 | yes     | up     |        | 100000       |             |



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification                                                  |
|------------------|---------------------------------------------------------------|
| 10.10.1000       | Added parameters: <b>&lt;COUNT&gt;</b> , <b>&lt;SPEED&gt;</b> |
| 10.07 or earlier | --                                                            |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## cdp

cdp

### Description

Configures CDP support globally on all active interfaces or on a specific interface. By default, CDP is enabled on all active interfaces.

When CDP is enabled, the switch adds entries to its CDP Neighbors table for any CDP packets it receives from neighboring CDP devices.

When CDP is disabled, the CDP Neighbors table is cleared and the switch drops all inbound CDP packets without entering the data in the CDP Neighbors table.

The **no** form of this command disables CDP support globally on all active interfaces or on a specific interface.

### Examples

Enabling CDP globally:

```
switch(config)# cdp
```

Disabling CDP globally:

```
switch(config)# no cdp
```

Enabling CDP on interface **1/1/1**:

```
switch(config)# interface 1/1/1s
switch(config-if)# cdp
```

Disabling CDP on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no cdp
```



---

For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

---

### Command History



| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | config<br>config-if | Administrators or local user group members with execution rights for this command. |

# clear cdp counters

clear cdp counters

## Description

Clears CDP counters.

## Examples

Clearing CDP counters:

```
switch(config) clear cdp counters
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# clear cdp neighbor-info

clear cdp neighbor-info

## Description

Clears CDP neighbor information.

## Examples

Clearing CDP neighbor information:

```
switch(config) clear neighbor-info
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show cdp

```
show cdp
```

### Description

Shows CDP information for all interfaces.

### Examples

Showing CDP information:

```
switch(config)# show cdp
CDP Global Information
=====
CDP : Enabled
CDP Mode : Rx only
CDP Hold Time : 180 seconds

Port CDP

1/1/1 Enabled
1/1/2 Enabled
1/1/3 Enabled
1/1/4 Enabled
1/1/5 Enabled
1/1/6 Enabled
1/1/7 Enabled
1/1/8 Enabled
1/1/9 Enabled
1/1/10 Enabled
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | config          | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show cdp neighbor-info

show cdp neighbor-info <INTERFACE-ID>

### Description

Shows CDP information for all neighbors or for CDP information on a specific interface.

| Parameter      | Description                                               |
|----------------|-----------------------------------------------------------|
| <INTERFACE-ID> | Specifies an interface. Format: <b>member/slot/port</b> . |

### Examples

Showing all CDP neighbor information:

```
switch(config)# show cdp neighbor-info
Total Neighbor Entries : 1
Port Device ID Platform Capability

1/1/1 HPE_ANW-3810M-24G-1-slot... HPE ANW Sw S
```

Showing CDP information for interface **1/1/1**:

```
switch(config)# show cdp neighbor-info 1/1/1
Local Port : 1/1/1
MAC : 70:10:6f:86:78:7f
Device ID : HPE_ANW-3810M-24G-1-slot(70106f-867800)
Address : 127.0.0.1
Platform : HPE ANW Sw
Duplex : half
Version : Revision KB.16.07.0002, ROM KB.16.01....
Capability : switch
Native VLAN : 1
Voice VLAN Support : No
Neighbor Port-ID : 1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | config          | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show cdp traffic

show cdp traffic

### Description

Shows CDP statistics for each interface.

### Examples

Showing CDP traffic statistics:

```
switch(config)# show cdp traffic
```

```
CDP Statistics
```

```
=====
```

| Port  | Transmitted Frames | Received Frames | Discarded Frames |
|-------|--------------------|-----------------|------------------|
| 1/1/1 | 0                  | 4               | 0                |
| 1/1/2 | 0                  | 0               | 0                |
| 1/1/3 | 0                  | 2               | 0                |
| 1/1/4 | 0                  | 0               | 0                |
| 1/1/5 | 0                  | 0               | 0                |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | config          | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show cdp voice-vlan mode

show cdp voice-vlan mode

## Description

Shows CDP voice-vlan and mode.

## Examples

Showing CDP voice-vlan and mode:

```
switch(config)# show cdp voice-vlan mode
CDP voice VLAN mode
=====
Port Voice VLAN Mode

1/1/1 N/A Rx only
1/1/2 N/A Rx only
1/1/3 N/A Rx only
1/1/4 N/A Rx only
1/1/5 N/A Rx only
1/1/6 N/A Rx only
1/1/7 N/A Rx only
1/1/8 N/A Rx only
1/1/9 N/A Rx only
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | config          | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

### checkpoint auto

checkpoint auto <TIME-LAPSE-INTERVAL>

#### Description

Starts auto checkpoint mode. In auto checkpoint mode, the switch temporarily saves the runtime configuration as a checkpoint only for the specified time lapse interval. Configuration changes must be saved before the interval expires, otherwise the runtime configuration is restored from the temporary checkpoint.

| Parameter             | Description                                                   |
|-----------------------|---------------------------------------------------------------|
| <TIME-LAPSE-INTERVAL> | Specifies the time lapse interval in minutes. Range: 1 to 60. |

#### Usage

To save the runtime checkpoint permanently, run the **checkpoint auto confirm** command during the time lapse interval. The filename for the saved checkpoint is named **AUTO <YYYYMMDDHHSS>**. If the **checkpoint auto confirm** command is not entered during the specified time lapse interval, the previous runtime configuration is restored.

#### Examples

Confirming the auto checkpoint:

```
switch# checkpoint auto 20
Auto checkpoint mode expires in 20 minute(s)
switch# WARNING Please "checkpoint auto confirm" within 2 minutes
switch# checkpoint auto confirm
checkpoint AUTO20170801011154 created
```

In this example, the runtime checkpoint was saved because the **checkpoint auto confirm** command was entered within the value set by the **time-lapse-interval** parameter, which was 20 minutes.

Not confirming the auto checkpoint:

```
switch# checkpoint auto 20
Auto checkpoint mode expires in 20 minute(s)
switch# WARNING Please "checkpoint auto confirm" within 2 minutes
WARNING: Restoring configuration. Do NOT add any new configuration.
Restoration successful
```

In this example, the runtime checkpoint was reverted because the **checkpoint auto confirm** command was not entered within the value set by the **time-lapse-interval** parameter, which was 20 minutes.



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# checkpoint auto confirm

checkpoint auto confirm

## Description

Signals to the switch to save the running configuration used during the auto checkpoint mode. This command also ends the auto checkpoint mode.

## Usage

To save the runtime checkpoint permanently, run the **checkpoint auto confirm** command during the time lapse value set by the **checkpoint auto TIME-LAPSE-INTERVAL** command. The generated checkpoint name will be in the format **AUTO <YYYYMMDDHHSS>**. If the **checkpoint auto confirm** command is not entered during the specified time lapse interval, the previous runtime configuration is restored.

## Examples

Confirming the auto checkpoint:

```
switch# checkpoint auto confirm
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## checkpoint diff

```
checkpoint diff {<CHECKPOINT-NAME1> | running-config | startup-config}
 {<CHECKPOINT-NAME2> | running-config | startup-config | REMOTE_URL | STORAGE_URL}
[vrf <VRF_NAME>] [deep]
```

### Description

Shows the difference in configuration between two configurations. Compare checkpoints, the running configuration, or the startup configuration.

| Parameter                                              | Description                                                                                           |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| {<CHECKPOINT-NAME1>   running-config   startup-config} | Selects either a checkpoint, the running configuration, or the startup configuration as the baseline. |
| {<CHECKPOINT-NAME2>   running-config   startup-config} | Selects either a checkpoint, the running configuration, or the startup configuration to compare.      |
| REMOTE_URL   STORAGE-URL                               | Retrieves a CLI type configuration from a remote or local file. Configurations must be in CLI format. |
| [vrf <VRF_NAME>]                                       | Specifies the VRF name when using a REMOTE_URL to download a checkpoint.                              |
| [deep]                                                 | Uses a deep mode comparison.                                                                          |

### Usage



REMOTE\_URL or STORAGE\_URL configurations must be in CLI format only, checkpoint format is currently not supported.

In order to get accurate diff results, ensure that the imported file has a valid configuration, correct indentation to represent context changes between CLI contexts, and the file uses the Unix end of line format (\n). The imported file should follow the same syntax and format as the output for **show running-config**. The use of 4 spaces is recommended over the use of tab.

When using the default diff mode, the output of a similar Unix **diff-u** is used. The deep option makes the comparison based on unique entries within a given context instead of based on the order of configuration lines.

The output of the **checkpoint diff** command has several symbols:

- The plus sign (+) at the beginning of a line indicates that the line exists in the comparison but not in the baseline.



- The minus sign (-) at the beginning of a line indicates that the line exists in the baseline but not in the comparison.
- An empty space ( ) is used to represent configuration contexts that exist in both configurations (common) but contain added or removed entries.

## Examples

In the following example, the configurations of checkpoints **cp1** and **cp2** are displayed before the **checkpoint diff** command, so that you can see the context of the **checkpoint diff** command.

```
switch# show checkpoint cp1
Checkpoint configuration:
!
!Version AOS-CX XL.10.00.0002
!Schema version 0.1.8
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1,200
interface 1/1/1
 no shutdown
 ip address 1.0.0.1/24
interface 1/1/2
 no shutdown
 ip address 2.0.0.1/24

switch# show checkpoint cp2
Checkpoint configuration:
!
!Version AOS-CX XL.10.00.0002
!Schema version 0.1.8
module 1/1 product-number jl363a
!
!
!
!
!
!
!
!
!
vlan 1,200,300
interface 1/1/1
 no shutdown
 ip address 1.0.0.1/24
interface 1/1/2
 no shutdown
 ip address 2.0.0.1/24

switch# checkpoint diff cp1 cp2
--- /tmp/chkpt11501550258421 2017-08-01 01:17:38.420514016 +0000
+++ /tmp/chkpt21501550258421 2017-08-01 01:17:38.420514016 +0000
@@ -9,7 +9,7 @@
!
!
!
-vlan 1,200
+vlan 1,200,300
```

```
interface 1/1/1
 no shutdown
 ip address 1.0.0.1/24
```

```
switch# checkpoint diff chkpt01 chkpt02
--- /tmp/chkpt011607564301327
+++ /tmp/chkpt021607564301353
@@ -1,7 +1,7 @@
!
!Version AOS-CX PL.10.06.0100V
!export-password: default
-hostname Switch
+hostname Switch1
 user admin group administrators password ciphertext
 AQBapTyg9tpaiAaTfSVV5eNdFzOORRvZ6CMpglh1P+LQUHQLYgAAAGAhmRqFbkNvrgy2SBVk7H8C5hvg/I
 ib8rWYFZLEaSCroBNP9EwMu+hLNM0xmsh45yG8dncP7WkxjwrW4p4Qra6dVfr0EW8xh/lpQf8F/2Wki20L
 c9JLXiYge7ti0H6cVn+G
 radius-server tracking interval 60
 no usb

switch#
```

Showing the difference in configuration between two configurations using the deep option.

```
switch# checkpoint diff running-config checkpoint run deep
-vlan 1, 100
+vlan 1
```

Showing the difference in configuration between two configurations using the deep option when there are warnings related to the file.

```
switch# checkpoint diff running-config sftp://user@172.17.0.1/config2.txt vrf mgmt
deep(user@172.17.0.1) Password:
sftp> get halon-src/hpe-config/scripts/configdiff/configdiff/config2.txt
userconfig2.txt
-vlan 1, 100
+vlan 1

WARN: Use of tabs is not recommended. File: dest-config2.txt line: 15
WARN: Use of tabs is not recommended. File: dest-config2.txt line: 16
```

Showing the difference in configuration between two configurations using the deep option when there are errors in the file and no diff output is displayed.

```
switch# checkpoint diff running-config sftp://user@172.17.0.1/config.txt vrf mgmt
deep(user@172.17.0.1) Password:
sftp> get config.txt userconfig.txt
ERROR: Duplicate entry found. File: dest-config.txt (line 25): 'vlan 2'
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                 |
|------------------|--------------------------------------------------------------|
| 10.16            | Updated syntax to include REMOTE_URL, STORAGE_URL, and deep. |
| 10.07 or earlier | --                                                           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# checkpoint post-configuration

`checkpoint post-configuration`

`no checkpoint post-configuration`

## Description

Enables creation of system generated checkpoints when configuration changes occur. This feature is enabled by default.

The **no** form of this command disables system generated checkpoints.

## Usage

System generated checkpoints are automatically created by default. Whenever a configuration change occurs, the switch starts a timeout counter (300 seconds by default). For each additional configuration change, the timeout counter is restarted. If the timeout expires with no additional configuration changes being made, the switch generates a new checkpoint.

System generated checkpoints are named with the prefix **CPC** followed by a time stamp in the format **<YYYYMMDDHHMMSS>**. For example: **CPC20170630073127**.

System checkpoints can be applied using the checkpoint rollback feature or copy command.

A maximum of 32 system checkpoints can be created. Beyond this limit, the newest system checkpoint replaces the oldest system checkpoint.

## Examples

Enabling system checkpoints:

```
switch(config)# checkpoint post-configuration
```

Disabling system checkpoints:

```
switch(config)# no checkpoint post-configuration
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# checkpoint post-configuration timeout

`checkpoint post-configuration timeout <TIMEOUT>`

`no checkpoint post-configuration timeout <TIMEOUT>`

## Description

Sets the timeout for the creation of system checkpoints. The timeout specifies the amount of time since the latest configuration for the switch to create a system checkpoint.

The **no** form of this command resets the timeout to 300 seconds, regardless of the value of the **<TIMEOUT>** parameter.

| Parameter                            | Description                                                      |
|--------------------------------------|------------------------------------------------------------------|
| <code>timeout &lt;TIMEOUT&gt;</code> | Specifies the timeout in seconds. Range: 5 to 600. Default: 300. |

## Examples

Setting the timeout for system checkpoints to 60 seconds:

```
switch(config)# checkpoint post-configuration timeout 60
```

Resetting the timeout for system checkpoints to 300 seconds:

```
switch(config)# no checkpoint post-configuration timeout 1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## checkpoint rename

`checkpoint rename <OLD-CHECKPOINT-NAME> <NEW-CHECKPOINT-NAME>`

### Description

Renames an existing checkpoint.

| Parameter                                | Description                                                                                                                                                                                                                                                          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;OLD-CHECKPOINT-NAME&gt;</code> | Specifies the name of an existing checkpoint to be renamed.                                                                                                                                                                                                          |
| <code>&lt;NEW-CHECKPOINT-NAME&gt;</code> | Specifies the new name for the checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-).<br><br><b>NOTE:</b><br>Do not start the checkpoint name with <b>CPC</b> because it is used for system-generated checkpoints. |

### Examples

Renaming checkpoint **ckpt1** to **cfg001**:

```
switch# checkpoint rename ckpt1 cfg001
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## checkpoint rollback

`checkpoint rollback {<CHECKPOINT-NAME> | startup-config}`

## Description

Applies the configuration from a pre-existing checkpoint or the startup configuration to the running configuration.

| Parameter                            | Description                          |
|--------------------------------------|--------------------------------------|
| <code>&lt;CHECKPOINT-NAME&gt;</code> | Specifies a checkpoint name.         |
| <code>startup-config</code>          | Specifies the startup configuration. |

## Examples

Applying a checkpoint named **ckpt1** to the running configuration:

```
switch# checkpoint rollback ckpt1
Success
```

Applying a startup checkpoint to the running configuration:

```
switch# checkpoint rollback startup-config
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## **copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL>**

`copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL> [vrf <VRF-NAME>]`

## Description

Copies a checkpoint configuration to a remote location as a file. The configuration is exported in checkpoint format, which includes switch configuration and relevant metadata.

| Parameter                            | Description                                                                                                                                                                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;CHECKPOINT-NAME&gt;</code> | Specifies the name of a checkpoint.                                                                                                                                                                                                                                                                    |
| <code>&lt;REMOTE-URL&gt;</code>      | Specifies the remote destination and filename using the syntax:<br><b>TFTP format:</b><br>tftp://<IP-ADDR>[:<PORT-NUM>]<br>[;blocksize=<Value>]/<FILENAME><br><b>SFTP format:</b><br>sftp://<USERNAME>@<IP-ADDR><br>[:<PORT-NUM>]/<FILENAME><br><b>SCP format:</b><br>scp://USER@{IP HOST}[:PORT]/FILE |
| <code>vrf &lt;VRF-NAME&gt;</code>    | Specifies a VRF name.                                                                                                                                                                                                                                                                                  |

## Examples

Copying checkpoint configuration to remote file through TFTP:

```
switch# copy checkpoint ckpt1 tftp://192.168.1.10/ckptmeta vrf default
100.0%
Success
```

Copying checkpoint configuration to remote file through SFTP:

```
switch# copy checkpoint ckpt1 sftp://root@192.168.1.10/ckptmeta vrf default
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ECDSA key fingerprint is SHA256:FtOm6Uxuxumil7VCwLnhz92H9LkjY+eURbdddOETy50.
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.1.10's password:
sftp> put /tmp/ckptmeta ckptmeta
Uploading /tmp/ckptmeta to /root/ckptmeta
Warning: Permanently added '192.168.1.10' (ECDSA) to the list of known hosts.
Connected to 192.168.1.10.
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy checkpoint <CHECKPOINT-NAME> {running-config | startup-config}

copy checkpoint <CHECKPOINT-NAME> {running-config | startup-config}

## Description

Copies an existing checkpoint configuration to the running configuration or to the startup configuration.

| Parameter         | Description                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <CHECKPOINT-NAME> | Specifies the name of an existing checkpoint.                                                                                                                                                                           |
|                   | Selects whether the running configuration or the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration. |

## Examples

Copying **ckpt1** checkpoint to the running configuration:

```
switch# copy checkpoint ckpt1 running-config
Success
```

Copying **ckpt1** checkpoint to the startup configuration:

```
switch# copy checkpoint ckpt1 startup-config
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>

copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>



## Description

Copies an existing checkpoint configuration to a USB drive. The file format is defined when the checkpoint was created.

| Parameter                            | Description                                                                                                                                                                    |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;CHECKPOINT-NAME&gt;</code> | Specifies the name of the checkpoint to copy. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-).                                     |
| <code>&lt;STORAGE-URL&gt;&gt;</code> | Specifies the name of the target file on the USB drive using the following syntax: <code>usb:/&lt;FILE&gt;</code><br>The USB drive must be formatted with the FAT file system. |

## Examples

Copying the **test** checkpoint to the **testCheck** file on the USB drive:

```
switch# copy checkpoint test usb:/testCheck
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## **copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME>**

`copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME> [vrf <VRF-NAME>]`

## Description

Copies a remote configuration file to a checkpoint. The remote configuration file must be in checkpoint format.

| Parameter                       | Description                                                                |
|---------------------------------|----------------------------------------------------------------------------|
| <code>&lt;REMOTE-URL&gt;</code> | Specifies a remote file using the following syntax:<br><b>TFTP format:</b> |

| Parameter         | Description                                                                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <pre>tftp://&lt;IP-ADDR&gt;[:&lt;PORT-NUM&gt;] [;blocksize=&lt;Value&gt;]/&lt;FILENAME&gt;</pre> <p><b>SFTP format:</b></p> <pre>sftp://&lt;USERNAME&gt;@&lt;IP-ADDR&gt; [:&lt;PORT-NUM&gt;]/&lt;FILENAME&gt;</pre> <p><b>SCP format:</b></p> <pre>scp://USER@{IP HOST}[:PORT]/FILE</pre>  |
| <CHECKPOINT-NAME> | <p>Specifies the name of the target checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-). Required.</p> <p><b>NOTE:</b> Do not start the checkpoint name with <code>CPC</code> because it is used for system-generated checkpoints.</p> |
| vrf <VRF-NAME>    | Specifies a VRF name. Default: default.                                                                                                                                                                                                                                                    |

## Examples

Copying a checkpoint format file to checkpoint **ckpt5** on the default VRF:

```
switch# copy tftp://192.168.1.10/ckptmeta checkpoint ckpt5
100.0%
100.0%
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy <REMOTE-URL> startup-config|running-config

```
copy <REMOTE-URL> startup-config|{running-config [overwrite]} [vrf <VRF-NAME>]
```

### Description

Copies a remote file containing a switch configuration to the running configuration or to the startup configuration.

| Parameter                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;REMOTE-URL&gt;</code>   | <p>Specifies a remote file with the following syntax:</p> <p><b>TFTP format:</b></p> <pre>tftp://&lt;IP-ADDR&gt;[:&lt;PORT-NUM&gt;] [;blocksize=&lt;Value&gt;]/&lt;FILENAME&gt;</pre> <p><b>SFTP format:</b></p> <pre>sftp://&lt;USERNAME&gt;@&lt;IP-ADDR&gt; [:&lt;PORT-NUM&gt;]/&lt;FILENAME&gt;</pre> <p><b>SCP format:</b></p> <pre>scp://USER@{IP HOST}[:PORT]/FILE</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>startup-config</code>       | Indicates that the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>running-config</code>       | Indicates that the running configuration receives the copied checkpoint configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>overwrite</code>            | <p>By default, the CLI configuration contained in the copied file is applied on top of the running-config, so the CLI command does not clear the running-config before applying the CLI commands. In the event that a particular CLI command fails then the failure is logged in event logs and the next line in CLI configuration is processed.</p> <p>When you include the <b>overwrite</b> parameter, the configuration is only applied to the running-config if <i>all</i> the commands succeeded without errors. If there are any errors during the copy process, the existing running-config will remain intact. You can then inspect the event logs to check and fix the errors and retry the operation. If more than 20 errors are present, the operation stops processing any further commands. The event logs will display only those errors processed up to that point.</p> |
| <code>vrf &lt;VRF-NAME&gt;</code> | Specifies the name of a VRF. Default: default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Usage

The switch copies only certain file types. The format of the file is automatically detected from contents of the file. The **startup-config** option only supports the JSON file format and checkpoints, but the **running-config** option supports the JSON and CLI file formats and checkpoints.

When a file of the CLI format is copied, it overwrites the running configuration. The CLI command does not clear the running configuration before applying the CLI commands. All of the CLI commands in the file are applied line-by-line. If a particular CLI command fails, the switch logs the failure and it continues to the next line in the CLI configuration. The event log (**show events -d hpe-config**) provides information as to which command failed.

## Examples

Copying a JSON format file to the running configuration:

```
switch# copy tftp://192.168.1.10/runjson running-config
100.0%
Configuration may take several minutes to complete according to configuration file
size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Success
```

Copying a CLI format file to the running configuration with an error in the file:

```
switch# copy tftp://192.168.1.10/runcli running-config
100.0%
Configuration may take several minutes to complete according to configuration file
size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Some of the configuration lines from the file were NOT applied. Use 'show
events -d hpe-config' for more info.
100.0%
Configuration may take several minutes to complete according to configuration file
size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Some of the configuration lines from the file were NOT applied. Use 'show
events -d hpe-config' for more info.
```

Copying a CLI format file to the startup configuration:

```
switch# copy tftp://192.168.1.10/startjson startup-config
100.0%
100.0%
Success
```

Copying an unsupported file format to the startup configuration:

```
switch# copy tftp://192.168.1.10/startfile startup-config
100.0%
100.0%
unsupported file format
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                           |
|------------------|----------------------------------------|
| 10.15            | The overwrite parameter is introduced. |
| 10.07 or earlier | --                                     |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>}

copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>}

## Description

Copies the running configuration to the startup configuration or to a new checkpoint. If the startup configuration is already present, the command overwrites the existing startup configuration.

| Parameter                                       | Description                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>startup-config</code>                     | Specifies that the startup configuration receives a copy of the running configuration.                                                                                                                                                                                                                                                               |
| <code>checkpoint &lt;CHECKPOINT-NAME&gt;</code> | Specifies the name of a new checkpoint to receive a copy of the running configuration. The checkpoint name can be comprised of alphanumeric character, underscores (_) and dashes (-), and must be 32 characters or fewer.<br><br><b>NOTE:</b> Do not start the checkpoint name with <b>CPC</b> because it is used for system-generated checkpoints. |

## Examples

Copying the running configuration to the startup configuration:

```
switch# copy running-config startup-config
Success
```

Copying the running configuration to a new checkpoint named **ckpt1**:

```
switch# copy running-config checkpoint ckpt1
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## `copy {running-config | startup-config} <REMOTE-URL>`

`copy {running-config | startup-config} <REMOTE-URL> {cli | json} [vrf <VRF-NAME>]`

## Description

Copies the running configuration or the startup configuration to a remote file in either CLI or JSON format.

| Parameter                         | Description                                                                                                                                                                                                                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {running-config   startup-config} | Selects whether the running configuration or the startup configuration is copied to a remote file.                                                                                                                                                                                       |
| <REMOTE-URL>                      | Specifies the remote file using the syntax:<br><b>TFTP format:</b><br>tftp://<IP-ADDR>[:<PORT-NUM>]<br>[;blocksize=<Value>] / <FILENAME><br><b>SFTP format:</b><br>sftp://<USERNAME>@<IP-ADDR><br>[:<PORT-NUM>] / <FILENAME><br><b>SCP format:</b><br>scp://USER@{IP HOST}[:PORT] / FILE |
| {cli   json}                      | Selects the remote file format: P: CLI or JSON.                                                                                                                                                                                                                                          |
| vrf <VRF-NAME>                    | Specifies the name of a VRF. Default: default.                                                                                                                                                                                                                                           |

## Examples

Copying a running configuration to a remote file in CLI format:

```
switch# copy running-config tftp://192.168.1.10/runcli cli
100.0%
Success
```

Copying a running configuration to a remote file in JSON format:

```
switch# copy running-config tftp://192.168.1.10/runjson json
100.0%
Success
```

Copying a startup configuration to a remote file in CLI format:

```
switch# copy startup-config sftp://root@192.168.1.10/startcli cli
root@192.168.1.10's password:
sftp> put /tmp/startcli startcli
Uploading /tmp/startcli to /root/startcli
Connected to 192.168.1.10.
Success
```

Copying a startup configuration to a remote file in JSON format:

```
switch# copy startup-config sftp://root@192.168.1.10/startjson json
root@192.168.1.10's password:
sftp>
root@192.168.1.10's password:
sftp> put /tmp/startjson startjson
Uploading /tmp/startjson to /root/startjson
Connected to 192.168.1.10.
```

Success



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy {running-config | startup-config} <STORAGE-URL>

copy {running-config | startup-config} <STORAGE-URL> {cli | json}

## Description

Copies the running configuration or a startup configuration to a USB drive.

| Parameter                         | Description                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------|
| {running-config   startup-config} | Selects the running configuration or the startup configuration to be copied to the switch USB drive. |
| <STORAGE-URL>                     | Specifies a remote file with the following syntax: <b>usb:/&lt;file&gt;</b>                          |
| {cli   json}                      | Selects the format of the remote file: CLI or JSON.                                                  |

## Usage

The switch supports JSON and CLI file formats when copying the running or starting configuration to the USB drive. The USB drive must be formatted with the FAT file system.

The USB drive must be enabled and mounted with the following commands:

```
switch(config)# usb
switch(config)# end
switch# usb mount
```

## Examples

Copying a running configuration to a file named **runCLI** on the USB drive:

```
switch# copy running-config usb:/runCLI cli
Success
```

Copying a startup configuration to a file named **startCLI** on the USB drive:

```
switch# copy startup-config usb:/startCLI cli
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy startup-config running-config

copy startup-config running-config

## Description

Copies the startup configuration to the running configuration.

## Examples

```
switch# copy startup-config running-config
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information



| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy <STORAGE-URL> running-config

copy <STORAGE-URL> {running-config | startup-config | checkpoint <CHECKPOINT-NAME>}

### Description

This command copies a specified configuration from the USB drive to the running configuration, to a startup configuration, or to a checkpoint.

| Parameter                    | Description                                                                                                                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <STORAGE-URL>                | Specifies the name of a configuration file on the USB drive with the syntax: <b>usb:/&lt;FILE&gt;</b>                                                                                                                                                                                                       |
| running-config               | Specifies that the configuration file is copied to the running configuration. The file must be in CLI, JSON, or checkpoint format or the copy will fail. the copy will not work.                                                                                                                            |
| startup-config               | Specifies that the configuration file is copied to the startup configuration. The switch stores this configuration between reboots. The startup configuration is used as the operating configuration following a reboot of the switch. The file must be in JSON or checkpoint format or the copy will fail. |
| checkpoint <CHECKPOINT-NAME> | Specifies the name of a new checkpoint file to receive a copy of the configuration. The configuration file on the USB drive must be in checkpoint format.<br><br><b>NOTE:</b><br>Do not start the checkpoint name with <b>CPC</b> because it is used for system-generated checkpoints.                      |

### Usage

This command requires that the USB drive is formatted with the FAT file system and that the file be in the appropriate format as follows:

- **running-config:** This option requires the file on the USB drive be in CLI, JSON, or checkpoint format.
- **startup-config:** This option requires the file on the USB drive be in JSON or checkpoint format.
- **checkpoint <checkpoint-name>:** This option requires the file on the USB drive be in checkpoint format.

### Examples

Copying the file **runCli** from the USB drive to the running configuration:

```
switch# copy usb:/runCli running-config
Configuration may take several minutes to complete according to configuration
file size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
```

Success

Copying the file **startUp** from the USB drive to the startup configuration:

```
switch# copy usb:/startUp startup-config
Success
```

Copying the file **testCheck** from the USB drive to the **abc** checkpoint:

```
switch# copy usb:/testCheck checkpoint abc
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## erase

```
erase
 checkpoint <checkpont-name>
 core-dump all|daemon|dsm|kernel
 startup-config
 all
```

## Description

Deletes an existing checkpoint, startup configuration, or core-dump.

| Parameter                                        | Description                                                                                                                                                                                                                                                       |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| checkpoint <CHECKPOINT-NAME>                     | Specifies the name of a checkpoint.                                                                                                                                                                                                                               |
| core-dump<br>all daemon <daemon-name><br> kernel | Erase one of the following sets of core-dump files: <ul style="list-style-type: none"><li>■ all: Erase all core-dump files.</li><li>■ daemon &lt;daemon-name&gt;: Erase daemon core-dump files.</li><li>■ kernel: Erase the kernel core-dump.</li><li>■</li></ul> |

| Parameter             | Description                          |
|-----------------------|--------------------------------------|
| <i>startup-config</i> | Specifies the startup configuration. |
| <i>all</i>            | Specifies all checkpoints.           |

## Examples

Erasing checkpoint **ckpt1**:

```
switch# erase checkpoint ckpt1
```

Erasing the startup configuration:

```
switch# erase startup-config
```

Erasing all checkpoints:

```
switch# erase checkpoint all
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show checkpoint <CHECKPOINT-NAME>

```
show checkpoint <CHECKPOINT-NAME> [json]
```

### Description

Shows the configuration of a checkpoint.

| Parameter         | Description                                            |
|-------------------|--------------------------------------------------------|
| <CHECKPOINT-NAME> | Specifies the name of a checkpoint.                    |
| [json]            | Specifies that the output is displayed in JSON format. |

## Examples

Showing the configuration of the **ckpt1** checkpoint in CLI format:

```
switch# show checkpoint ckpt1
Checkpoint configuration:
!
!Version AOS-CX PL.10.07.0000K-75-g55e5193
!export-password: default
lacp system-priority 65535
user admin group administrators password ciphertext
AQBapQjwipbev36io0jFfde7ZzrHckncallD+3n8XFTZKQdmYgAAADetYOeHSme93xzdD0uz6Vr9Kl+XBz
B+2GB0UBxSF7rvqN2x8KSgkqv7iqXVQ0Te6LkSMnH4BdNaT3Bf25qyvOqmr4YakO1V3rg8zAOADkPktQD8
joTHXflzwomoIzcmv/uX
cli-session
 timeout 0
!
!
!
!
ssh server vrf default
vlan 1
spanning-tree
interface lag 1
 no shutdown
 vlan access 1
interface lag 128
 no shutdown
 vlan access 1
interface lag 129
 shutdown
 vlan access 1
 lacp mode active
interface 1/1/1
 no shutdown
 lag 128
 lacp port-id 65535
interface 1/1/2
 no shutdown
 vlan access 1
interface 1/1/3
 no shutdown
 vlan access 1
interface 1/1/4
 no shutdown
 vlan access 1
interface 1/1/5
 no shutdown
 vlan access 1
interface 1/1/6
 no shutdown
 vlan access 1
interface 1/1/7
 no shutdown
 vlan access 1
interface 1/1/8
 no shutdown
 vlan access 1
interface 1/1/9
 no shutdown
 vlan access 1
interface 1/1/10
 no shutdown
```

```

 vlan access 1
interface 1/1/11
 no shutdown
 vlan access 1
interface 1/1/12
 no shutdown
 vlan access 1
interface 1/1/13
 no shutdown
 vlan access 1
interface 1/1/14
 no shutdown
 vlan access 1
interface 1/1/15
 no shutdown
 vlan access 1
interface 1/1/16
 no shutdown
 vlan access 1
interface vlan 1
 ip dhcp
snmp-server vrf default
!
!
!
!
!
https-server vrf default

```

Showing the configuration of the **ckpt1** checkpoint in JSON format:

```

switch# show checkpoint ckpt1 json
Checkpoint configuration:
{
 "AAA_Server_Group": {
 "local": {
 "group_name": "local"
 },
 "none": {
 "group_name": "none"
 }
 },
 ...
 ...
 ...
 ...

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show checkpoint <CHECKPOINT-NAME> hash

show checkpoint <CHECKPOINT-NAME> hash [cli | json]

### Description

Shows a configuration checkpoint hash calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

| Parameter         | Description                            |
|-------------------|----------------------------------------|
| <CHECKPOINT-NAME> | Specifies an existing checkpoint name. |
| [cli   json]      | Selects either the CLI or JSON format. |

### Examples

Showing a checkpoint SHA-256 hash in JSON format:

```
switch# show checkpoint ckpt1 hash json
Calculating the hash: [Success]

The SHA-256 hash of the checkpoint in JSON format, created in image XX.10.08.xxxx:

cc7a57a9bbb4e6600d3b4180296a35f6af9e797ce9c439955dfe5de58b06da9e

This hash is only valid for comparison to a baseline hash if the configuration has
not been explicitly changed (such as with a CLI command, REST operation, etc.)
or implicitly changed (such as by changing a hardware module, upgrading the
SW version, etc.).
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show checkpoint post-configuration

show checkpoint post-configuration

## Description

Shows the configuration settings for creating system checkpoints.

## Examples

```
switch# show checkpoint post-configuration

Checkpoint Post-Configuration feature

Status : enabled
Timeout (sec) : 300
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show checkpoint

show checkpoint

## Description

Shows a detailed list of all saved checkpoints.

## Examples

Showing a detailed list of all saved checkpoints:

```
switch# show checkpoint

NAME TYPE WRITER DATE (YYYY/MM/DD) IMAGE VERSION
ckpt1 checkpoint User 2017-02-23T00:10:02Z XX.01.01.000X
ckpt2 checkpoint User 2017-03-08T18:10:01Z XX.01.01.000X
ckpt3 checkpoint User 2017-03-09T23:11:02Z XX.01.01.000X
ckpt4 checkpoint User 2017-03-11T00:00:03Z XX.01.01.000X
ckpt5 latest User 2017-03-14T01:12:27Z XX.01.01.000X
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                                                         |
|------------------|------------------------------------------------------------------------------------------------------|
| 10.08            | Command syntax <code>show checkpoint list all</code> is replaced with <code>show checkpoint</code> . |
| 10.07 or earlier | --                                                                                                   |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show checkpoint date

`show checkpoint date <START-DATE> <END-DATE>`

## Description

Shows detailed list of all saved checkpoints created within the specified date range.

| Parameter                       | Description                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------|
| <code>&lt;START-DATE&gt;</code> | Specifies the starting date for the range of saved checkpoints to show. Format: <b>YYYY-MM-DD</b> . |
| <code>&lt;END-DATE&gt;</code>   | Specifies the ending date for the range of saved checkpoints to show. Format: <b>YYYY-MM-DD</b> .   |

## Examples

Showing a detailed list of saved checkpoints for a specific date range:

```
switch# show checkpoint date 2017-03-08 2017-03-12
```

| NAME  | TYPE       | WRITER | DATE (YYYY/MM/DD)    | IMAGE         | VERSION |
|-------|------------|--------|----------------------|---------------|---------|
| ckpt2 | checkpoint | User   | 2017-03-08T18:10:01Z | XX.01.01.000X |         |
| ckpt3 | checkpoint | User   | 2017-03-09T23:11:02Z | XX.01.01.000X |         |
| ckpt4 | checkpoint | User   | 2017-03-11T00:00:03Z | XX.01.01.000X |         |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History



| Release          | Modification                                                                                                                                                                     |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.08            | Command syntax <code>show checkpoint list date &lt;START-DATE&gt; &lt;END-DATE&gt;</code> is replaced with <code>show checkpoint date &lt;START-DATE&gt; &lt;END-DATE&gt;</code> |
| 10.07 or earlier | --                                                                                                                                                                               |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show running-config hash

`show running-config hash [cli | json]`

### Description

Shows the running-config checkpoint hash, calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

| Parameter    | Description                            |
|--------------|----------------------------------------|
| [cli   json] | Selects either the CLI or JSON format. |

### Examples

Showing the running-config checkpoint SHA-256 hash in CLI format:

```
switch# show running-config hash cli
Calculating the hash: [Success]

SHA-256 hash of the config in CLI format:

8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62aa1d715075b89e

This hash is only valid for comparison to a baseline hash if the configuration has
not been explicitly changed (such as with a CLI command, REST operation, etc.)
or implicitly changed (such as by changing a hardware module, upgrading the
SW version, etc.).
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show startup-config hash

```
show startup-config hash [cli | json]
```

### Description

Shows the startup-config checkpoint hash, calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

| Parameter    | Description                            |
|--------------|----------------------------------------|
| [cli   json] | Selects either the CLI or JSON format. |

### Examples

Showing the startup-config checkpoint SHA-256 hash in CLI format:

```
switch# show startup-config hash cli
Calculating the hash: [Success]

SHA-256 hash of the config in CLI format:

8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62aa1d715075b89e

This hash is only valid for comparison to a baseline hash if the configuration has
not been explicitly changed (such as with a CLI command, REST operation, etc.)
or implicitly changed (such as by changing a hardware module, upgrading the
SW version, etc.).
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# write memory

write memory

## Description

Saves the running configuration to the startup configuration. It is an alias of the command **copy running-config startup-config**. If the startup configuration is already present, this command overwrites the startup configuration.

## Examples

```
switch# write memory
Success
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### Classifier policy application

Classifier policies can be applied as follows ("Rt-In" = "Routed-In"):

| Policy type<br>Direction         | IPv4+6<br>In | IPv4+6<br>Rt-In | MAC<br>In |
|----------------------------------|--------------|-----------------|-----------|
| L2 interface (port)              | Yes          |                 | Yes       |
| L2 LAG                           | Yes          |                 | Yes       |
| L3 interface (port)              | Yes          | Yes             | Yes       |
| L3 LAG                           | Yes          | Yes             | Yes       |
| L3 interface (port) subinterface | Yes          | Yes             | Yes       |
| L3 LAG subinterface              | Yes          | Yes             | Yes       |
| VLAN                             | Yes          |                 | Yes       |
| Interface VLAN                   |              | Yes (PBR)       |           |

Policies cannot match multicast packets on the routed in direction.

The following match criteria are not supported. If any of these match criteria are attempted to be configured, an error message will be displayed and the action will not be completed.

HPE Aruba Networking 8320, 8325, 9300/9300S, 10000 Switch Series:



TCP flags CWR and ECE  
TCP flags and TTL (hop limit) on IP classes  
Fragment on IPv6 classes in VLAN policies  
VLAN ID in VLAN policies

HPE Aruba Networking 8320 Switch Series only:

IPv4 AH on inbound classes

### apply policy (config-if, config-lag-if, config-if-vlan, config-vlan)

**Context config-if, config-lag-if:**

```
apply policy <POLICY-NAME> {in|out|routed-in} [per-interface]
```

```
no apply policy <POLICY-NAME> {in|out|routed-in} [per-interface]
```

### Context config-vlan:

```
apply policy <POLICY-NAME> {in|out}
no apply policy <POLICY-NAME> {in|out}
```

### Context config-if-vlan:

```
apply policy <POLICY-NAME> routed-in
no apply policy <POLICY-NAME> routed-in
```

## Description

Applies a policy to the current physical interface port or LAG or VLAN context.

Only one direction of a policy can be applied to an interface or VLAN at a time, thus using the apply command on an interface or VLAN with an already-applied policy of the same direction will replace the currently applied policy.



The VLAN context supports the **in** and **out** directions, which apply to both bridged and routed traffic. The Interface VLAN context only supports the **routed-in** direction which applies only to routed traffic.

The **no** form of this command removes a policy from the interface or VLAN specified by the current context.

| Parameter     | Description                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POLICY-NAME> | Specifies the policy to apply.                                                                                                                                  |
| in            | Selects the inbound (ingress) traffic direction.                                                                                                                |
| out           | Selects the outbound (egress) traffic direction.                                                                                                                |
| routed-in     | Selects routed in traffic.                                                                                                                                      |
| per-interface | Specifies that unique instances of the policy be applied to each interface or LAG rather than the default of sharing the policy across all interfaces and LAGs. |

## Usage (applies to *config-if*, *config-lag-if* contexts)

- Subinterfaces only support the ingress (**in** and **routed-in**) directions. Ingress on subinterfaces is supported on the HPE Aruba Networking 8325 and 10000 Switch series but not on the HPE Aruba Networking 8320, 9300, 9300S Switch series.
- When **per-interface** is included, unique instances of the policy are applied to each physical interface port or LAG rather than the default of sharing the policy across all interfaces and LAGs. The unique instance of a policy has a parent-child relationship with the policy from which it was created. The **per-interface** option is useful when you want unique policers to be created for each interface or LAG rather than using shared policers. It is also useful when you want the statistics (hit counts and conform rate) to be specific to an interface or LAG rather than being aggregated. Because **per-interface** creates more hardware instances of a policy, resource consumption may increase significantly. It is recommended that you use **show resources** to monitor resource utilization as configuration is applied.

## Usage (applies to config-vlan context)

- Only one policy type may be applied to a VLAN at a time. Therefore, using the **apply policy** command on a VLAN with an already-applied policy of the same type, will replace the applied policy.

## Examples

Applying a policy to an interface (ingress):

```
switch(config)# interface 1/1/1
switch(config-if)# apply policy MY_POLICY1 in
```

Applying a policy to an interface (ingress) specifying **per-interface**:

```
switch(config)# interface 1/1/2
switch(config-if)# apply policy MY_POLICY1 in per-interface
```

Applying a policy to an interface (egress):

```
switch(config)# interface 1/1/2
switch(config-if)# apply policy MY_POLICY2 out
```

Applying a policy to an interface (egress) specifying **per-interface**:

```
switch(config)# interface 1/1/2
switch(config-if)# apply policy MY_POLICY2 out per-interface
```

Applying a policy to an interface range (ingress):

```
switch(config)# interface 1/1/3-1/1/6
switch(config-if-<1/1/2-1/1/5>)# apply policy MY_POLICY3 in
```

Applying a policy to an interface range (ingress) specifying **per-interface**:

```
switch(config)# interface 1/1/7-1/1/9
switch(config-if-<1/1/2-1/1/5>)# apply policy MY_POLICY4 in per-interface
```

Removing a policy from an interface (ingress):

```
switch(config)# interface 1/1/1
switch(config-if)# no apply policy MY_POLICY1 in
```

Removing a policy from an interface range (ingress):

```
switch(config)# interface 1/1/3-1/1/6
switch(config-if-<1/1/3-1/1/6>)# no apply policy MY_POLICY3 in
```

Applying a policy to a LAG (ingress):

```
switch(config)# interface lag 100
switch(config-lag-if)# apply policy MY_POLICY5 in
```

Applying a policy to a LAG (ingress) specifying **per-interface**:

```
switch(config)# interface lag 200
switch(config-lag-if)# apply policy MY_POLICY5 in per-interface
```

Removing a policy from a LAG (ingress):

```
switch(config)# interface lag 100
switch(config-lag-if)# no apply policy MY_POLICY5 in
```

Applying a policy to a VLAN (ingress):

```
switch(config)# vlan 1
switch(config-vlan)# apply policy MY_POLICY6 in
```

Applying a policy to a VLAN (egress):

```
switch(config)# vlan 1
switch(config-vlan)# no apply policy my_policy out
```

Applying a policy to multiple VLANs (ingress):

```
switch(config)# vlan 10,20
switch(config-vlan-<10,20>)# apply policy MY_POLICY7 in
```

Applying a policy to an interface VLAN routed (ingress):

```
switch(config)# vlan 1
switch(config-if-vlan)# apply policy MY_POLICY8 routed-in
```

Applying a policy to an interface VLAN range routed (ingress):

```
switch(config)# vlan 2-5
switch(config-if-vlan-<2-5>)# apply policy MY_POLICY8 routed-in
```

Removing a policy from a VLAN (ingress):

```
switch(config)# vlan 1
switch(config-vlan)# no apply policy MY_POLICY6 in
```

Removing a policy from multiple VLANs (ingress):

```
switch(config)# vlan 10,20
switch(config-vlan-<10,20>)# no apply policy MY_POLICY7 in
```

Removing a policy from an interface VLAN routed (ingress):

```
switch(config)# vlan 1
switch(config-if-vlan)# no apply policy MY_POLICY8 routed-in
```

Removing a policy from an interface VLAN range routed (ingress):

```
switch(config)# vlan 2-5
switch(config-if-vlan-<2-5>)# no apply policy MY_POLICY8 routed-in
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                             | Authority                                                                          |
|---------------|-------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if<br>config-lag-if<br>config-vlan<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## apply policy

```
apply policy <POLICY-NAME> {in}
no apply policy <POLICY-NAME> {in}
```

### Description

Applies a policy to the global config context.

Only one policy can be globally applied at a time. Applying a policy globally again, replaces the previous globally applied policy.

The **no** form of this command removes application of the global policy.

| Parameter     | Description                                      |
|---------------|--------------------------------------------------|
| <POLICY-NAME> | Specifies the policy to apply.                   |
| in            | Selects the inbound (ingress) traffic direction. |



## Examples

Applying policy global1 to the global config context:

```
switch(config)# apply policy global1 in
```

Removing application of policy global1 from the global config context:

```
switch(config)# no apply policy global1 in
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## class copy

```
class {ip|ipv6|mac} <CLASS-NAME> copy <DESTINATION-CLASS>
```

### Description

Copies a class to a new destination class or overwrites an existing class. Copying a class copies all entries as well.

| Parameter                  | Description                                            |
|----------------------------|--------------------------------------------------------|
| {ip ipv6 mac} <CLASS-NAME> | Specifies the type and name of the class to be copied. |
| <DESTINATION-CLASS>        | Specifies the name of the destination class.           |

## Examples

Copying an IPv4 class. Copying a class with entries copies all its entries as well:

```
switch(config)# class ip MY_IP_CLASS copy MY_IP_CLASS2
switch(config)# do show class
Type Name
Sequence Comment
Action
L3 Protocol
```

|       |    | Source IP Address      | Source L4 Port(s)      |
|-------|----|------------------------|------------------------|
|       |    | Destination IP Address | Destination L4 Port(s) |
|       |    | Additional Parameters  |                        |
| ----- |    |                        |                        |
| IPv4  |    | MY_IP_CLASS            |                        |
|       | 11 | ignore                 | udp                    |
|       |    | any                    |                        |
|       |    | any                    |                        |
|       | 21 | match                  | tcp                    |
|       |    | 192.168.0.1            |                        |
|       |    | 192.168.0.2            |                        |
| ----- |    |                        |                        |
| IPv4  |    | MY_IP_CLASS2           |                        |
|       | 11 | ignore                 | udp                    |
|       |    | any                    |                        |
|       |    | any                    |                        |
|       | 21 | match                  | tcp                    |
|       |    | 192.168.0.1            |                        |
|       |    | 192.168.0.2            |                        |

Copying an IPv6 class:

```
switch(config)# class ipv6 MY_IPV6_CLASS copy MY_IPV6_CLASS2
switch(config)# do show class
Type Name
Sequence Comment
Action
Source IP Address L3 Protocol
Destination IP Address Source L4 Port(s)
Additional Parameters Destination L4 Port(s)

IPv6 MY_IPV6_CLASS
2 ignore
any
any
udp

IPv6 MY_IPV6_CLASS2
2 ignore
any
any
udp
```

Copying a MAC class:

```
switch(config)# class mac MY_MAC_CLASS copy MY_MAC_CLASS2
switch(config)# do show class
Type Name
Sequence Comment
Action
Source MAC Address EtherType
Destination MAC Address
Additional Parameters

MAC MY_MAC_CLASS
2 ignore
any
any
arp

MAC MY_MAC_CLASS2
2 ignore
any
arp
```

```
any
any
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## class ip

Syntax to create an IPv4 class and enter its context. Plus syntax to remove a class:

```
class ip <CLASS-NAME>
no class ip <CLASS-NAME>
```

Syntax (within the class context) for creating or removing class entries for protocols **ah**, **gre**, **esp**, **igmp**, **ospf**, **pim** (**ip** is available as an alias for **any**):

```
[<SEQUENCE-NUMBER>]
{match|ignore}
{any|ip|ah|gre|esp|igmp|ospf|pim|<IP-PROTOCOL-NUM>}
{any|<SRC-IP-ADDRESS>[/ {<PREFIX-LENGTH>|<SUBNET-MASK>}]}
{any|<DST-IP-ADDRESS>[/ {<PREFIX-LENGTH>|<SUBNET-MASK>}]}
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count]

no <SEQUENCE-NUMBER>
```

Syntax (within the class context) for creating or removing class entries for protocols **sctp**, **tcp**, **udp**:

```
[<SEQUENCE-NUMBER>]
{match|ignore}
{sctp|tcp|udp}
{any|<SRC-IP-ADDRESS>[/ {<PREFIX-LENGTH>|<SUBNET-MASK>}]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
{any|<DST-IP-ADDRESS>[/ {<PREFIX-LENGTH>|<SUBNET-MASK>}]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
[cwr][ece][urg][ack][psh][rst][syn][fin][established]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count]

no <SEQUENCE-NUMBER>
```

Syntax (within the class context) for creating or removing class entries for protocol **icmp**:

```
[<SEQUENCE-NUMBER>]
{match|ignore}
{icmp}
{any|<SRC-IP-ADDRESS>[/ {<PREFIX-LENGTH>|<SUBNET-MASK>}]}
{any|<DST-IP-ADDRESS>[/ {<PREFIX-LENGTH>|<SUBNET-MASK>}]}
```

```
[icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count]
```

```
no <SEQUENCE-NUMBER>
```

Syntax (within the class context) for class entry comments:

```
[<SEQUENCE-NUMBER>] comment <TEXT-STRING>
```

```
no <SEQUENCE-NUMBER> comment
```

## Description

Creates or modifies an IPv4 traffic class to match specified packets. Class is composed of one or more class entries ordered and prioritized by sequence numbers. With this command, the class can classify traffic based on IPv4 header information.

The **no** form of the command can be used to delete either an IPv4 traffic class (use **no** with the class command) or an individual IPv4 traffic class entry (use **no** with the sequence number).

| Parameter                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip                                                              | Specifies create or modify an IPv4 class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <CLASS-NAME>                                                    | Specifies the name of this class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <SEQUENCE-NUMBER>                                               | Specifies a sequence number for the class entry. Optional. Range: 1-4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| {match ignore}                                                  | Creates a rule to match or ignore specified packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <IP-PROTOCOL-NUM>                                               | Specifies the protocol as its Internet Protocol number. For example, 2 corresponds to the IGMP protocol. Range: 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                          |
| {any <SRC-IP-ADDRESS><br>[/ {<PREFIX-LENGTH> <SUBNET-MASK>} ] } | Specifies the source IPv4 address. <ul style="list-style-type: none"> <li>▪ <b>any</b> - specifies any source IPv4 address.</li> <li>▪ <b>&lt;SRC-IP-ADDRESS&gt;</b> - specifies the source IPv4 host address. <ul style="list-style-type: none"> <li>◦ <b>&lt;PREFIX-LENGTH&gt;</b> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32.</li> <li>◦ <b>&lt;SUBNET-MASK&gt;</b> - specifies the address bits to mask (dotted decimal notation).</li> </ul> </li> </ul>                |
| {any <DST-IP-ADDRESS><br>[/ {<PREFIX-LENGTH> <SUBNET-MASK>} ] } | Specifies the destination IPv4 address. <ul style="list-style-type: none"> <li>▪ <b>any</b> - specifies any destination IPv4 address.</li> <li>▪ <b>&lt;DST-IP-ADDRESS&gt;</b> - specifies the destination IPv4 host address. <ul style="list-style-type: none"> <li>◦ <b>&lt;PREFIX-LENGTH&gt;</b> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32.</li> <li>◦ <b>&lt;SUBNET-MASK&gt;</b> - specifies the address bits to mask (dotted decimal notation).</li> </ul> </li> </ul> |

| Parameter                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>[{eq gt lt} &lt;PORT&gt; range &lt;MIN-PORT&gt;&lt;MAX-PORT&gt;]</code> | <p>Specifies the port or port range. Port numbers are in the range of 0 to 65535.</p> <ul style="list-style-type: none"> <li>▪ <b>eq &lt;PORT&gt;</b> - specifies the Layer 4 port.</li> <li>▪ <b>gt &lt;PORT&gt;</b> - specifies any Layer 4 port greater than the indicated port.</li> <li>▪ <b>lt &lt;PORT&gt;</b> - specifies any Layer 4 port less than the indicated port.</li> <li>▪ <b>range &lt;MIN-PORT&gt; &lt;MAX-PORT&gt;</b> - specifies the Layer 4 port range.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| <code>cwr</code>                                                              | Specifies matching on the TCP Flag CWR : Congestion Window Reduced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>ece</code>                                                              | Specifies matching on the TCP Flag ECE : Explicit Congestion Notification [ECN]- Echo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>urg</code>                                                              | Specifies matching on the TCP Flag: Urgent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>ack</code>                                                              | Specifies matching on the TCP Flag: Acknowledgment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>psh</code>                                                              | Specifies matching on the TCP Flag: Push buffered data to receiving application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <code>rst</code>                                                              | Specifies matching on the TCP Flag: Reset the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>syn</code>                                                              | Specifies matching on the TCP Flag: Synchronize sequence numbers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>fin</code>                                                              | Specifies matching on the TCP Flag: Finish connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>established</code>                                                      | Specifies matching on the TCP Flag: Established connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>dscp &lt;DSCP-SPECIFIER&gt;</code>                                      | <p>Specifies the Differentiated Services Code Point (DSCP), either a numeric <b>&lt;DSCP-VALUE&gt;</b> (0 to 63) or one of these keywords:</p> <ul style="list-style-type: none"> <li>▪ <b>AF11</b> - DSCP 10 (Assured Forwarding Class 1, low drop probability)</li> <li>▪ <b>AF12</b> - DSCP 12 (Assured Forwarding Class 1, medium drop probability)</li> <li>▪ <b>AF13</b> - DSCP 14 (Assured Forwarding Class 1, high drop probability)</li> <li>▪ <b>AF21</b> - DSCP 18 (Assured Forwarding Class 2, low drop probability)</li> <li>▪ <b>AF22</b> - DSCP 20 (Assured Forwarding Class 2, medium drop probability)</li> <li>▪ <b>AF23</b> - DSCP 22 (Assured Forwarding Class 2, high drop probability)</li> <li>▪ <b>AF31</b> - DSCP 26 (Assured Forwarding Class 3, low drop probability)</li> </ul> |

| Parameter                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <ul style="list-style-type: none"> <li>▪ <b>AF32</b> - DSCP 28 (Assured Forwarding Class 3, medium drop probability)</li> <li>▪ <b>AF33</b> - DSCP 30 (Assured Forwarding Class 3, high drop probability)</li> <li>▪ <b>AF41</b> - DSCP 34 (Assured Forwarding Class 4, low drop probability)</li> <li>▪ <b>AF42</b> - DSCP 36 (Assured Forwarding Class 4, medium drop probability)</li> <li>▪ <b>AF43</b> - DSCP 38 (Assured Forwarding Class 4, high drop probability)</li> <li>▪ <b>CS0</b> - DSCP 0 (Class Selector 0: Default)</li> <li>▪ <b>CS1</b> - DSCP 8 (Class Selector 1: Scavenger)</li> <li>▪ <b>CS2</b> - DSCP 16 (Class Selector 2: OAM)</li> <li>▪ <b>CS3</b> - DSCP 24 (Class Selector 3: Signaling)</li> <li>▪ <b>CS4</b> - DSCP 32 (Class Selector 4: Realtime)</li> <li>▪ <b>CS5</b> - DSCP 40 (Class Selector 5: Broadcast video)</li> <li>▪ <b>CS6</b> - DSCP 48 (Class Selector 6: Network control)</li> <li>▪ <b>CS7</b> - DSCP 56 (Class Selector 7)</li> <li>▪ <b>EF</b> - DSCP 46 (Expedited Forwarding)</li> </ul> |
| ecn <ECN-VALUE>                           | Specifies an Explicit Congestion Notification value. Range: 0 to 3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ip-precedence <IP-PRECEDENCE-VALUE>       | Specifies an IP precedence value. Range: 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| tos <TOS-VALUE>                           | Specifies the Type of Service value. Range: 0 to 31.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| fragment                                  | Specifies a fragment packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| vlan <VLAN-ID>                            | <p>Specifies VLAN tag to match on. 802.1Q VLAN ID.</p> <p><b>NOTE:</b><br/>This parameter cannot be used in any class that will be applied to a VLAN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ttl <TTL-VALUE>                           | Specifies a time-to-live (hop limit) value. Range: 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| count                                     | Keeps the hit counts of the number of packets matching this class entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| [<SEQUENCE-NUMBER>] comment <TEXT-STRING> | Adds a comment to a class entry. The <b>no</b> form removes only the comment from the class entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Usage

- Entering an existing <CLASS-NAME> value will cause the existing class to be modified, with any new <SEQUENCE-NUMBER> value creating an additional class entry, and any existing <SEQUENCE-

**NUMBER>** value replacing the existing class entry with the same sequence number.

- If no sequence number is specified, a new class entry will be appended to the end of the class with a sequence number equal to the highest class entry currently in the list plus 10.
- If the **<IP-PROTOCOL-NUM>** parameter is used instead of a protocol name, ensure that any needed class entry-definition parameters specific to the selected protocol are also provided.

The following match criteria are not supported for use in egress policies on HPE Aruba Networking 9300, 9300S Switch series:

- **TTL** (hop limit)

## Examples

Creating an IPv4 class with three entries:

```
switch(config)# class ip MY_IP_CLASS
switch(config-class-ip) # 10 match icmp any any10 match icmp any any
switch(config-class-ip) # 20 ignore udp any any
switch(config-class-ip) # 30 match tcp 192.168.0.1 192.168.0.2
switch(config-class-ip) # exit

switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv4 MY_IP_CLASS
 10 match
 any
 any
 20 ignore
 any
 any
 30 match
 192.168.0.1
 192.168.0.2
 L3 Protocol
 Source L4 Port(s)
 Destination L4 Port(s)
```

Adding a comment to an existing IPv4 class entry:

```
switch(config)# class ip MY_IP_CLASS
switch(config-class-ip) # 30 comment myipClass
switch(config-class-ip) # exit

switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv4 MY_IP_CLASS
 10 match
 any
 any
 30 match
 192.168.0.1
 192.168.0.2
 L3 Protocol
 Source L4 Port(s)
 Destination L4 Port(s)
```

```

20 ignore udp
 any
 any
30 myipClass
 match tcp
 192.168.0.1
 192.168.0.2

```

Removing a comment from an existing IPv4 class entry:

```

switch(config)# class ip MY_IP_CLASS
switch(config-class-ip)# no 30 comment
switch(config-class-ip)# exit

```

```

switch(config)# do show class

```

| Type     | Name    |                        |                        |
|----------|---------|------------------------|------------------------|
| Sequence | Comment | Action                 | L3 Protocol            |
|          |         | Source IP Address      | Source L4 Port(s)      |
|          |         | Destination IP Address | Destination L4 Port(s) |
|          |         | Additional Parameters  |                        |

```

IPv4 MY_IP_CLASS
10 match
 any
 any
20 ignore
 any
 any
30 match
 192.168.0.1
 192.168.0.2

```

| Type     | Name    |                        |                        |
|----------|---------|------------------------|------------------------|
| Sequence | Comment | Action                 | L3 Protocol            |
|          |         | Source IP Address      | Source L4 Port(s)      |
|          |         | Destination IP Address | Destination L4 Port(s) |
|          |         | Additional Parameters  |                        |

```

IPv4 MY_IP_CLASS
10 match
 any
 any
20 ignore
 any
 any
30 match
 192.168.0.1
 192.168.0.2

```

Replacing an IPv4 class entry in an existing class:

```

switch(config)# class ip MY_IP_CLASS
switch(config-class-ip)# 10 match igmp any any
switch(config-class-ip)# exit

```

```

switch(config)# do show class

```

| Type | Name |
|------|------|
|------|------|



| Sequence | Comment                |  |                        |
|----------|------------------------|--|------------------------|
|          | Action                 |  | L3 Protocol            |
|          | Source IP Address      |  | Source L4 Port(s)      |
|          | Destination IP Address |  | Destination L4 Port(s) |
|          | Additional Parameters  |  |                        |
| -----    |                        |  |                        |
| IPv4     | MY_IP_CLASS            |  |                        |
| 10       | match                  |  | igmp                   |
|          | any                    |  |                        |
|          | any                    |  |                        |
| 20       | ignore                 |  | udp                    |
|          | any                    |  |                        |
|          | any                    |  |                        |
| 30       | match                  |  | tcp                    |
|          | 192.168.0.1            |  |                        |
|          | 192.168.0.2            |  |                        |

Removing an IPv4 class entry:

```
switch(config)# class ip MY_IP_CLASS
switch(config-class-ip)# no 10
switch(config-class-ip)# exit

switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv4 MY_IP_CLASS
20 ignore
 any
 any
30 match
 192.168.0.1
 192.168.0.2
 L3 Protocol
 Source L4 Port(s)
 Destination L4 Port(s)
```

Removing an IPv4 class. Removing a class with entries removes all its entries as well. If a class associated with a policy entry (or multiple policy entries) is removed, the corresponding entries are also removed.



The corresponding entries are only removed if the class is unused by all policy entries.

```
switch(config)# no class ip MY_IP_CLASS

switch(config)# do show class
No Class found.
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                                                                                                              | Authority                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | <b>config</b><br><b>The class ip &lt;CLASS-NAME&gt; command takes you into the config-class-ipconfig-class-ip context where you enter the class entries.</b> | Administrators or local user group members with execution rights for this command. |

## class ipv6

Syntax to create an IPv6 class and enter its context. Plus syntax to remove a class:

```
class ipv6 <CLASS-NAME>
no class ipv6 <CLASS-NAME>
```

Syntax (within the class context) for creating or removing class entries for protocols ah, gre, esp, igmp, ospf, pim (ipv6 is available as an alias for any):

```
[<SEQUENCE-NUMBER>]
{match|ignore}
{any|ipv6|ah|gre|esp|igmp|ospf|pim|<IP-PROTOCOL-NUM>}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]]}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]]}
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count]

no <SEQUENCE-NUMBER>
```

Syntax (within the class context) for creating or removing class entries for protocols sctp, tcp, udp:

```
[<SEQUENCE-NUMBER>]
{match|ignore}
{sctp|tcp|udp}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
[urg] [ack] [psh] [rst] [syn] [fin] [established]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count]

no <SEQUENCE-NUMBER>
```

Syntax (within the class context) for creating or removing class entries for protocol icmpv6:

```
[<SEQUENCE-NUMBER>]
{permit|deny}
{icmpv6}
{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]]}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>|<SUBNET-MASK>]]}
[icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
[dscp <DSCP-SPECIFIER>] [ecn <ECN-VALUE>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [ttl <TTL-VALUE>] [count]
```

no <SEQUENCE-NUMBER>

Syntax (within the class context) for class entry comments:

[<SEQUENCE-NUMBER>] comment <TEXT-STRING>

no <SEQUENCE-NUMBER> comment

## Description

Creates or modifies an IPv6 traffic class to match specified packets. Class is composed of one or more class entries ordered and prioritized by sequence numbers. With this command, each class can classify traffic based on IPv6 header information.

The **no** form of the command deletes either an IPv6 traffic class (use **no** with the class command) or an individual IPv6 traffic class entry (use **no** with the sequence number).

| Parameter                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6                                                               | Specifies create or modify an IPv6 class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <CLASS-NAME>                                                       | Specifies the name of this class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <SEQUENCE-NUMBER>                                                  | Specifies a sequence number for the class entry. Optional. Range: 1-4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| {match ignore}                                                     | Creates a rule to match or ignore specified packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <IP-PROTOCOL-NUM>                                                  | Specifies the protocol as its Internet Protocol number. For example, 2 corresponds to the IGMP protocol. Range: 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                  |
| {any <SRC-IP-ADDRESS>[/<br>{<br><PREFIX-LENGTH> <SUBNET-MASK>}]} } | Specifies the source IPv6 address. <ul style="list-style-type: none"><li>▪ <b>any</b> - specifies any source IPv6 address.</li><li>▪ <b>&lt;SRC-IP-ADDRESS&gt;</b> - specifies the source IPv4 host address.<ul style="list-style-type: none"><li>◦ <b>&lt;PREFIX-LENGTH&gt;</b> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32.</li><li>◦ <b>&lt;SUBNET-MASK&gt;</b> - specifies the address bits to mask (dotted decimal notation).</li></ul></li></ul>                |
| {any <DST-IP-ADDRESS>[/<br>{<br><PREFIX-LENGTH> <SUBNET-MASK>}]} } | Specifies the destination IPv4 address. <ul style="list-style-type: none"><li>▪ <b>any</b> - specifies any destination IPv6 address.</li><li>▪ <b>&lt;DST-IP-ADDRESS&gt;</b> - specifies the destination IPv6 host address.<ul style="list-style-type: none"><li>◦ <b>&lt;PREFIX-LENGTH&gt;</b> - specifies the address bits to mask (CIDR subnet mask notation). Range: 1 to 32.</li><li>◦ <b>&lt;SUBNET-MASK&gt;</b> - specifies the address bits to mask (dotted decimal notation).</li></ul></li></ul> |
| [{eq gt lt} <PORT> range<br><MIN-PORT><MAX-PORT>]                  | Specifies the port or port range. Port numbers are in the range of 0 to 65535. <ul style="list-style-type: none"><li>▪ <b>eq &lt;PORT&gt;</b> - specifies the Layer 4 port.</li></ul>                                                                                                                                                                                                                                                                                                                      |

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <ul style="list-style-type: none"> <li>▪ <b>gt &lt;PORT&gt;</b> - specifies any Layer 4 port greater than the indicated port.</li> <li>▪ <b>lt &lt;PORT&gt;</b> - specifies any Layer 4 port less than the indicated port.</li> <li>▪ <b>range &lt;MIN-PORT&gt; &lt;MAX-PORT&gt;</b> - specifies the Layer 4 port range.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| cwr                   | Specifies matching on the TCP Flag CWR : Congestion Window Reduced                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ece                   | Specifies matching on the TCP Flag ECE : Explicit Congestion Notification [ECN]- Echo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| urg                   | Specifies matching on the TCP Flag: Urgent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ack                   | Specifies matching on the TCP Flag: Acknowledgment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| psh                   | Specifies matching on the TCP Flag: Push buffered data to receiving application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| rst                   | Specifies matching on the TCP Flag: Reset the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| syn                   | Specifies matching on the TCP Flag: Synchronize sequence numbers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| fin                   | Specifies matching on the TCP Flag: Finish connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| established           | Specifies matching on the TCP Flag: Established connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| dscp <DSCP-SPECIFIER> | <p>Specifies the Differentiated Services Code Point (DSCP), either a numeric &lt;DSCP-VALUE&gt; (0 to 63) or one of these keywords:</p> <ul style="list-style-type: none"> <li>▪ <b>AF11</b> - DSCP 10 (Assured Forwarding Class 1, low drop probability)</li> <li>▪ <b>AF12</b> - DSCP 12 (Assured Forwarding Class 1, medium drop probability)</li> <li>▪ <b>AF13</b> - DSCP 14 (Assured Forwarding Class 1, high drop probability)</li> <li>▪ <b>AF21</b> - DSCP 18 (Assured Forwarding Class 2, low drop probability)</li> <li>▪ <b>AF22</b> - DSCP 20 (Assured Forwarding Class 2, medium drop probability)</li> <li>▪ <b>AF23</b> - DSCP 22 (Assured Forwarding Class 2, high drop probability)</li> <li>▪ <b>AF31</b> - DSCP 26 (Assured Forwarding Class 3, low drop probability)</li> <li>▪ <b>AF32</b> - DSCP 28 (Assured Forwarding Class 3, medium drop probability)</li> </ul> |

| Parameter                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <ul style="list-style-type: none"> <li>▪ <b>AF33</b> - DSCP 30 (Assured Forwarding Class 3, high drop probability)</li> <li>▪ <b>AF41</b> - DSCP 34 (Assured Forwarding Class 4, low drop probability)</li> <li>▪ <b>AF42</b> - DSCP 36 (Assured Forwarding Class 4, medium drop probability)</li> <li>▪ <b>AF43</b> - DSCP 38 (Assured Forwarding Class 4, high drop probability)</li> <li>▪ <b>CS0</b> - DSCP 0 (Class Selector 0: Default)</li> <li>▪ <b>CS1</b> - DSCP 8 (Class Selector 1: Scavenger)</li> <li>▪ <b>CS2</b> - DSCP 16 (Class Selector 2: OAM)</li> <li>▪ <b>CS3</b> - DSCP 24 (Class Selector 3: Signaling)</li> <li>▪ <b>CS4</b> - DSCP 32 (Class Selector 4: Real time)</li> <li>▪ <b>CS5</b> - DSCP 40 (Class Selector 5: Broadcast video)</li> <li>▪ <b>CS6</b> - DSCP 48 (Class Selector 6: Network control)</li> <li>▪ <b>CS7</b> - DSCP 56 (Class Selector 7)</li> <li>▪ <b>EF</b> - DSCP 46 (Expedited Forwarding)</li> </ul> |
| ecn <ECN-VALUE>                           | Specifies an Explicit Congestion Notification value. Range: 0 to 3.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ip-precedence <IP-PRECEDENCE-VALUE>       | Specifies an IP precedence value. Range: 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| tos <TOS-VALUE>                           | Specifies the Type of Service value. Range: 0 to 31.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| fragment                                  | Specifies a fragment packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| vlan <VLAN-ID>                            | <p>Specifies VLAN tag to match on. 802.1Q VLAN ID.</p> <p><b>NOTE:</b><br/>This parameter cannot be used in any class that will be applied to a VLAN.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ttl <TTL-VALUE>                           | Specifies a time-to-live (hop limit) value. Range: 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| count                                     | Keeps the hit counts of the number of packets matching this class entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| [<SEQUENCE-NUMBER>] comment <TEXT-STRING> | Adds a comment to a class entry. The <b>no</b> form removes only the comment from the class entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Usage

- If you enter an existing **<CLASS-NAME>** value, the existing class is modified with any new **<SEQUENCE-NUMBER>** value. This action creates an additional class entry. Any existing **<SEQUENCE-NUMBER>** value replaces the existing class entry with the same sequence number.
- If no sequence number is specified, a new class entry is appended to the end of the class with a sequence number equal to the highest class entry currently in the list plus 10.
- If the **<IP-PROTOCOL-NUM>** parameter is used instead of a protocol name, ensure that any needed class entry-definition parameters specific to the selected protocol are also provided.

The following match criteria are not supported for use in egress policies on HPE Aruba Networking 9300, 9300S Switch series:

- **TTL** (hop limit)

## Examples

Creating an IPv6 class with two entries:

```
switch(config)# class ipv6 MY_IPV6_CLASS
switch(config-class-ipv6)# 10 match icmpv6 any any
switch(config-class-ipv6)# 20 ignore udp any any
switch(config-class-ipv6)# exit

switch(config)# do show class
Type Name
Sequence Comment
 Action L3 Protocol
 Source IP Address Source L4 Port(s)
 Destination IP Address Destination L4 Port(s)
 Additional Parameters

IPv6 MY_IPV6_CLASS
 10 match icmpv6
 any
 any
 20 ignore udp
 any
 any
```

Adding a comment to an existing IPv6 class entry:

```
switch(config)# class ipv6 MY_IPV6_CLASS
switch(config-class-ipv6)# 10 match icmpv6 any any
switch(config-class-ipv6)# 20 ignore udp any any
switch(config-class-ipv6)# 20 comment myipv6class
switch(config-class-ipv6)# exit

switch(config)# do show class
Type Name
Sequence Comment
 Action L3 Protocol
 Source IP Address Source L4 Port(s)
 Destination IP Address Destination L4 Port(s)
 Additional Parameters

IPv6 MY_IPV6_CLASS
 10 match icmpv6
 any
 any
 20 myipv6class
 ignore udp
 any
 any
```

Removing a comment from an existing IPv6 class entry:

```

switch(config)# class ipv6 MY_IPV6_CLASS
switch(config-class-ipv6)# no 20 comment
switch(config-class-ipv6)# exit

switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv6 MY_IPV6_CLASS
10 match
 any
 any
20 ignore
 any
 any

Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv6 MY_IPV6_CLASS
10 match
 any
 any
20 ignore
 any
 any

```

Replacing an IPv6 class entry in an existing IPv6 class:

```

switch(config)# class ipv6 MY_IPV6_CLASS
switch(config-class-ipv6)# 10 match any 1020::
switch(config-class-ipv6)# exit

switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv6 MY_IPV6_CLASS
10 match
 any
 1020::
20 ignore
 any
 any

```

Removing an IPv6 class entry:

```

switch(config)# class ipv6 MY_IPV6_CLASS
switch(config-class-ipv6)# no 10
switch(config-class-ipv6)# exit

switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv6 MY_IPV6_CLASS
20 ignore
any
any
 L3 Protocol
 Source L4 Port(s)
 Destination L4 Port(s)

```

Removing an IPv6 class. Removing a class with entries removes all its entries as well. If a class associated with a policy entry (or multiple policy entries) is removed, the corresponding entries are also removed.




---

The corresponding entries are only removed if the class is unused by all policy entries.

---

```

switch(config)# no class ipv6 MY_IPV6_CLASS

switch(config)# do show class
No Class found.

```




---

For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                                                                                                           | Authority                                                                          |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config<br>The <b>class ipv6 &lt;CLASS-NAME&gt;</b> command takes you into the <b>config-class-ipv6</b> command context where you enter the class entries. | Administrators or local user group members with execution rights for this command. |

## class mac

```

class mac <CLASS-NAME>

[<SEQUENCE-NUMBER>]

```



```

{match|ignore}
{any|<SRC-MAC-ADDRESS>[/<ETHERNET-MASK>]}
{any|<DST-MAC-ADDRESS>[/<ETHERNET-MASK>]}
{any|arp|appletalk|arp|fcoe|fcoe-init|ip|ipv6|ipx-arpa|ipx-non-arpa|is-is|
 lldp|mpls-multicast|mpls-unicast|q-in-q|rbridge|trill|wake-on-lan|
 <NUMERIC-ETHERTYPE>}
[pcp <PCP-VALUE>] [vlan <VLAN-ID>] [count]

[<SEQUENCE-NUMBER>] comment <TEXT-STRING>

```

## Description

Creates or modifies a MAC traffic class to match specified packets. Class is composed of one or more class entries ordered and prioritized by sequence numbers. With this command, each class can classify traffic based on MAC header information.

The **no** form of the command can be used to delete either a MAC traffic class (use **no** with the class command) or an individual MAC traffic class entry (use **no** with the sequence number).

| Parameter                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac                                       | Specifies create or modify a MAC class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <CLASS-NAME>                              | Specifies the name of this class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <SEQUENCE-NUMBER>                         | Specifies a sequence number for the class entry. Optional. Range: 1-4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| {match ignore}                            | Creates a rule to match or ignore specified packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| comment                                   | Stores the remaining entered text as a class comment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| {any <SRC-MAC-ADDRESS>[/<ETHERNET-MASK>]} | Specifies the source host MAC address (xxxx.xxxx.xxxx), OUI, or the keyword <b>any</b> . You can optionally include the following:<br><b>&lt;ETHERNET-MASK&gt;</b> - The address bits to mask (xxxx.xxxx.xxxx).                                                                                                                                                                                                                                                                                                                                                                                                                    |
| {any <DST-MAC-ADDRESS>[/<ETHERNET-MASK>]} | Specifies the destination host MAC address (xxxx.xxxx.xxxx), OUI, or the keyword <b>any</b> . You can optionally include the following:<br><b>&lt;ETHERNET-MASK&gt;</b> - The address bits to mask (xxxx.xxxx.xxxx).                                                                                                                                                                                                                                                                                                                                                                                                               |
| Protocol                                  | Select an ethertype protocol from the following (enter one only): <ul style="list-style-type: none"> <li>▪ <b>any</b> - Any ethertype protocol</li> <li>▪ <b>&lt;NUMERIC-ETHERTYPE&gt;</b> - Enter an EtherType protocol number. Range: 0x600-0xffff.</li> <li>▪ Or enter an EtherType protocol name from the following list:               <ul style="list-style-type: none"> <li>◦ <b>aarp</b></li> <li>◦ <b>appletalk</b></li> <li>◦ <b>arp</b></li> <li>◦ <b>fcoe</b></li> <li>◦ <b>fcoe-init</b></li> <li>◦ <b>ip</b></li> <li>◦ <b>ipv6</b></li> <li>◦ <b>ipx-arpa</b></li> <li>◦ <b>ipx-non-arpa</b></li> </ul> </li> </ul> |

| Parameter       | Description                                                                                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | <ul style="list-style-type: none"> <li>◦ <b>is-is</b></li> <li>◦ <b>lldp</b></li> <li>◦ <b>mpls-multicast</b></li> <li>◦ <b>mpls-unicast</b></li> <li>◦ <b>q-in-q</b></li> <li>◦ <b>rbridge</b></li> <li>◦ <b>trill</b></li> <li>◦ <b>wake-on-lan</b></li> </ul> |
| pcp <PCP-VALUE> | Specifies matching on QoS Priority Code Point. Range: 0-7.                                                                                                                                                                                                       |
| vlan <VLAN-ID>  | Specifies matching on a VLAN ID. Enter a VLAN ID or the VLAN name, if configured.<br><br><b>NOTE:</b><br>This parameter cannot be used in any class that will be applied to a VLAN.                                                                              |
| count           | Keeps the hit counts of the number of packets matching this class entry.                                                                                                                                                                                         |

## Examples

Creating a MAC class:

```
switch(config)# class mac MY_MAC_CLASS
switch(config-class-mac)# match any any lldp
switch(config-class-mac)# ignore any any arp
switch(config-class-mac)# exit
switch(config)# do show class
```

| Type  | Name         | Sequence | Action                  | Comment | EtherType |
|-------|--------------|----------|-------------------------|---------|-----------|
|       |              |          | Source MAC Address      |         |           |
|       |              |          | Destination MAC Address |         |           |
|       |              |          | Additional Parameters   |         |           |
| ----- |              |          |                         |         |           |
| MAC   | MY_MAC_CLASS |          |                         |         |           |
|       |              | 10       | match                   |         | lldp      |
|       |              |          | any                     |         |           |
|       |              |          | any                     |         |           |
|       |              | 20       | ignore                  |         | arp       |
|       |              |          | any                     |         |           |
|       |              |          | any                     |         |           |

Adding a comment to an existing MAC class entry:

```
switch(config)# class mac MY_MAC_CLASS
switch(config-class-mac)# 10 comment MY_CLASS_ENTRY10 comment MY_CLASS_ENTRY
switch(config-class-mac)# exit
switch(config)# do show class
```

| Type  | Name         | Sequence | Comment        | Action                  | EtherType |
|-------|--------------|----------|----------------|-------------------------|-----------|
|       |              |          |                | Source MAC Address      |           |
|       |              |          |                | Destination MAC Address |           |
|       |              |          |                | Additional Parameters   |           |
| ----- |              |          |                |                         |           |
| MAC   | MY_MAC_CLASS |          |                |                         |           |
|       |              | 10       | MY_CLASS_ENTRY | match                   | lldp      |
|       |              |          |                | any                     |           |
|       |              |          |                | any                     |           |
|       |              | 20       | ignore         |                         | arp       |
|       |              |          |                | any                     |           |
|       |              |          |                | any                     |           |

Removing a comment from an existing MAC class entry:

```
switch(config)# class mac MY_MAC_CLASS
switch(config-class-mac)# no 10 comment MY_CLASS_ENTRY
switch(config-class-mac)# exit
switch(config)# do show class
```

| Type  | Name         | Sequence | Comment | Action                  | EtherType |
|-------|--------------|----------|---------|-------------------------|-----------|
|       |              |          |         | Source MAC Address      |           |
|       |              |          |         | Destination MAC Address |           |
|       |              |          |         | Additional Parameters   |           |
| ----- |              |          |         |                         |           |
| MAC   | MY_MAC_CLASS |          |         |                         |           |
|       |              | 10       | match   |                         | lldp      |
|       |              |          |         | any                     |           |
|       |              |          |         | any                     |           |
|       |              | 20       | ignore  |                         | arp       |
|       |              |          |         | any                     |           |
|       |              |          |         | any                     |           |

Replacing a MAC class entry in an existing MAC class:

```
switch(config)# class mac MY_MAC_CLASS
switch(config-class-mac)# 10 match any any any
switch(config-class-mac)# exit
switch(config)# do show class
```

| Type  | Name         | Sequence | Comment | Action                  | EtherType |
|-------|--------------|----------|---------|-------------------------|-----------|
|       |              |          |         | Source MAC Address      |           |
|       |              |          |         | Destination MAC Address |           |
|       |              |          |         | Additional Parameters   |           |
| ----- |              |          |         |                         |           |
| MAC   | MY_MAC_CLASS |          |         |                         |           |
|       |              | 10       | match   |                         | any       |
|       |              |          |         | any                     |           |
|       |              |          |         | any                     |           |
|       |              | 20       | ignore  |                         | arp       |
|       |              |          |         | any                     |           |
|       |              |          |         | any                     |           |

Removing a MAC class entry:

```

switch(config)# class mac MY_MAC_CLASS
switch(config-class-mac)# no 1
switch(config-class-mac)# exit
switch(config)# do show class
Type Name
Sequence Comment
Action
Source MAC Address
Destination MAC Address
Additional Parameters

MAC MY_MAC_CLASS
 2 ignore
 any
 any
 arp

```

Removing a MAC class. Removing a class with entries removes all its entries as well. If a class associated with a policy entry (or multiple policy entries) is removed, the corresponding entries are also removed.




---

The corresponding entries are only removed if the class is unused by all policy entries.

---

```

switch(config)# no class mac MY_MAC_CLASS
switch(config)# do show class
No Class found.

```




---

For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                                                                                                 | Authority                                                                          |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>The <b>class mac &lt;CLASS-NAME&gt;</b> command takes you into the <b>config-class-mac</b> context where you enter the class entries. | Administrators or local user group members with execution rights for this command. |

## class resequence

```
class {ip|ipv6|mac} <CLASS-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>
```

### Description

Resequencing numbering in an IPv4, or IPv6, or MAC class.

| Parameter                                      | Description                                                     |
|------------------------------------------------|-----------------------------------------------------------------|
| <b>{ip ipv6 mac}</b> <i>&lt;CLASS-NAME&gt;</i> | Specifies the class where you want to resequence class entries. |
| <i>&lt;STARTING-SEQUENCE-NUMBER&gt;</i>        | Specifies the sequence number to start resequencing from.       |
| <i>&lt;INCREMENT&gt;</i>                       | Specifies how much to increment the sequence numbers by.        |

## Examples

Resequencing an IPv4 class:

```
switch(config)# class ip MY_IP_CLASS resequence 1 10
switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv4 MY_IP_CLASS
1 match
 any
 any
11 ignore
 any
 any
21 match
 192.168.0.1
 192.168.0.2
 L3 Protocol
 Source L4 Port(s)
 Destination L4 Port(s)
```

Resequencing an IPv6 class:

```
switch(config)# class ipv6 MY_IPV6_CLASS resequence 1 1
switch(config-class-ipv6)# exit
switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source IP Address
 Destination IP Address
 Additional Parameters

IPv6 MY_IPV6_CLASS
1 match
 any
 1020::
2 ignore
 any
 any
 L3 Protocol
 Source L4 Port(s)
 Destination L4 Port(s)
```

Resequencing a MAC class:

```
switch(config)# class mac MY_MAC_CLASS resequence 1 1
switch(config)# do show class
Type Name
Sequence Comment
 Action
 Source MAC Address
 Destination MAC Address
 Additional Parameters

MAC MY_MAC_CLASS
1 match any
 any
2 ignore arp
 any
 any
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## class reset

```
class { all | ip <CLASS-NAME> | ipv6 <CLASS-NAME> | mac <CLASS-NAME> } reset
```

### Description

Changes the user-specified class configuration to match the active class configuration. Use this command when there is a discrepancy between what the user configured and what is active and accepted by the system.

| Parameter                                                        | Description                                                                                                                                                                 |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| { all   ip <CLASS-NAME>   ipv6 <CLASS-NAME>   mac <CLASS-NAME> } | Specifies either <b>all</b> classes be reset or specifies the type ( <b>ip</b> for IPv4, <b>ipv6</b> for IPv6 or <b>mac</b> for MAC ACL) and name of the class to be reset. |

## Examples

Resetting the user-specified configuration to the active configuration:

```
switch(config)# class all reset
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## clear policy hitcounts

```
clear policy hitcounts { all | [<POLICY-NAME>] [[interface <IF-NAME> [in|routed-in]] |
[vlan <VLAN-ID> [in]]] | global }
```

## Description

Clears the policy hit count statistics.

| Parameter           | Description                                                                            |
|---------------------|----------------------------------------------------------------------------------------|
| all                 | Selects all policies.                                                                  |
| <POLICY-NAME>       | Specifies the policy name.                                                             |
| interface <IF-NAME> | Specifies the interface name.                                                          |
| vlan <VLAN-ID>      | Specifies the VLAN.                                                                    |
| in                  | Specifies the inbound (ingress) traffic direction.                                     |
| routed-in           | Selects the routed in traffic direction. Not applicable to a policy applied to a VLAN. |
| global              | Selects the globally applied policy.                                                   |

## Examples

Clearing policy hit counts and then showing the policy hit counts (statistics):

```
switch# clear policy hitcounts my_policy int 1/1/1 in
switch# show policy hitcounts my_policy
Statistics for Policy my_policy:
Interface 1/1/1* (in):
 Hit Count Configuration
10 class ipv6 my_class1 action dscp af21 action drop
 0 10 match any any any count
* policy statistics are shared among each context type (interface, VLAN).
 For routed ingress, they are only shared within the same VRF.
 Use 'policy NAME copy' to create a new policy for separate statistics.
```

Clearing the globally applied policy hit counts and then showing the global policy hit counts (statistics):

```
switch# clear policy hitcounts global
switch# show policy hitcounts global
Statistics for Policy global:
Global Policy:
 Hit Count Configuration
10 class ipv6 my_class1 action mirror
 0 10 match any any any count
* policy statistics are shared among each context type (interface, VLAN).
 For routed ingress, they are only shared within the same VRF.
 Use 'policy NAME copy' to create a new policy for separate statistics.
```

Clearing hit counts for policy **MY\_IPv6\_Policy** applied to VLAN 10 (ingress):

```
switch# clear policy hitcounts My_IPv6_Policy vlan 10 in
```

Clearing hit counts for all policies:

```
switch# clear policy hitcounts all
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |



# policy

policy <POLICY-NAME>

```
[<SEQUENCE-NUMBER>]
class {ip|ipv6|mac} <CLASS-NAME>
 action {<REMARK-ACTIONS> | <POLICE-ACTIONS> | <OTHER-ACTIONS>}
 [{<REMARK-ACTIONS> | <POLICE-ACTIONS> | <OTHER-ACTIONS>}]

[<SEQUENCE-NUMBER>]
comment ...
```

## Description

Creates or modifies classifier policy and policy entries. A policy is made up of one or more policy entries ordered and prioritized by sequence numbers. Each entry has an IPv4/IPv6/MAC class and zero or more policy actions associated with it.

A policy must be applied using the **apply** command.

The **no** form of the command can be used to delete either a policy (use **no** with the policy command) or an individual policy entry (use **no** with the sequence number).

| Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POLICY-NAME>                       | Specifies the name of the policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <SEQUENCE-NUMBER>                   | Specifies a sequence number for the policy entry. Optional. Range: 1 to 4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| comment                             | Stores the remaining entered text as a policy entry comment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| class {ip ipv6 mac} <CLASS-NAME>    | Specifies a type of class, <b>ip</b> for IPv4, <b>ipv6</b> for IPv6 and <b>mac</b> for a MAC policy. And specifies a class name.                                                                                                                                                                                                                                                                                                                                                                                               |
| <REMARK-ACTIONS>                    | Remark actions can be any of the following options:<br>{pcp <PRIORITY>   <b>ip-precedence</b> <IP-PRECEDENCE-VALUE>   dscp <DSCP-VALUE>   local-priority <LOCAL-PRIORITY-VALUE>} where:                                                                                                                                                                                                                                                                                                                                        |
| pcp <PCP-VALUE>                     | Specifies the Priority Code Point (PCP) value. Range: 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ip-precedence <IP-PRECEDENCE-VALUE> | Specifies the numeric IP precedence value. Range: 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| dscp <DSCP-VALUE>                   | Specifies a Differentiated Services Code Point (DSCP) value. Enter either a numeric value (0 to 63) or a keyword as follows: <ul style="list-style-type: none"><li>■ <b>AF11</b> - DSCP 10 (Assured Forwarding Class 1, low drop probability)</li><li>■</li><li>■ <b>AF12</b> - DSCP 12 (Assured Forwarding Class 1, medium drop probability)</li><li>■ <b>AF13</b> - DSCP 14 (Assured Forwarding Class 1, high drop probability)</li><li>■ <b>AF21</b> - DSCP 18 (Assured Forwarding Class 2, low drop probability)</li></ul> |

| Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | <ul style="list-style-type: none"> <li>▪ <b>AF22</b> - DSCP 20 (Assured Forwarding Class 2, medium drop probability)</li> <li>▪ <b>AF23</b> - DSCP 22 (Assured Forwarding Class 2, high drop probability)</li> <li>▪ <b>AF31</b> - DSCP 26 (Assured Forwarding Class 3, low drop probability)</li> <li>▪ <b>AF32</b> - DSCP 28 (Assured Forwarding Class 3, medium drop probability)</li> <li>▪ <b>AF33</b> - DSCP 30 (Assured Forwarding Class 3, high drop probability)</li> <li>▪ <b>AF41</b> - DSCP 34 (Assured Forwarding Class 4, low drop probability)</li> <li>▪ <b>AF42</b> - DSCP 36 (Assured Forwarding Class 4, medium drop probability)</li> <li>▪ <b>AF43</b> - DSCP 38 (Assured Forwarding Class 4, high drop probability)</li> <li>▪ <b>CS0</b> - DSCP 0 (Class Selector 0: Default)</li> <li>▪ <b>CS1</b> - DSCP 8 (Class Selector 1: Scavenger)</li> <li>▪ <b>CS2</b> - DSCP 16 (Class Selector 2: OAM)</li> <li>▪ <b>CS3</b> - DSCP 24 (Class Selector 3: Signaling)</li> <li>▪ <b>CS4</b> - DSCP 32 (Class Selector 4: Real time)</li> <li>▪ <b>CS5</b> - DSCP 40 (Class Selector 5: Broadcast video)</li> <li>▪ <b>CS6</b> - DSCP 48 (Class Selector 6: Network control)</li> <li>▪ <b>CS7</b> - DSCP 56 (Class Selector 7)</li> <li>▪ <b>EF</b> - DSCP 46 (Expedited Forwarding)</li> </ul> |
| local-priority <LOCAL-PRIORITY-VALUE> | Specifies a local priority value. Range: 0 to 7.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <POLICE-ACTIONS>                      | Police actions can be the following {cir <RATE-BPS>cbs <BYTES> exceed} where:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| cir kbps <RATE-KBPS>                  | Specifies a Committed Information Rate value in Kilobits per second. Range: 1 to 4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cbs <BYTES>                           | Specifies a Committed Burst Size value in bytes. Range: 1 to 4294967295.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <OTHER-ACTIONS>                       | Other actions can be the following:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| drop                                  | Specifies drop traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Usage

- An applied policy will process a packet sequentially against policy entries in the list until the last policy entry in the list has been evaluated or the packet matches an entry.
- Entering an existing <POLICY-NAME> value will cause the existing policy to be modified, with any new <SEQUENCE-NUMBER> value creating an additional policy entry, and any existing <SEQUENCE-NUMBER> value replacing the existing policy entry with the same sequence number.
- If no sequence number is specified, a new policy entry will be appended to the end of the entry list with a sequence number equal to the highest policy entry currently in the list plus 10.

## Examples

Creating a policy with several entries:

```
switch(config)# policy MY_POLICY
switch(config-policy)# 10 class ipv6 MY_CLASS1 action dscp af21 action drop
switch(config-policy)# 20 class ip MY_CLASS3 action mirror 1
switch(config-policy)# exit
switch(config)# show policy
 Name
Sequence Comment
 Class Type
 action

 MY_POLICY
10 MY_CLASS1 ipv6
 drop
 dscp AF21

20
 MY_CLASS3 ipv4
 mirror 1
```

Adding a comment to an existing policy entry:

```
switch(config)# policy MY_POLICY
switch(config-policy)# 20 comment MY_TEST_POLICY
switch(config-policy)# exit
switch(config)# show policy
 Name Sequence Comment Class Type action

MY_POLICY 10
 20 MY_TEST_POLICY MY_CLASS3 ipv4 mirror 1
MY_POLICY 10 MY_CLASS1 ipv6 drop dscp AF21
```

Removing a comment from an existing policy entry:

```
switch(config)# policy MY_POLICY
switch(config-policy)# no 20 comment
switch(config-policy)# exit
switch(config)# show policy
 Name Sequence Comment Class Type action

MY_POLICY 10
 20
MY_POLICY 10 MY_CLASS1 ipv6 drop dscp AF21
 20 MY_CLASS3 ipv4 mirror 1
```

Adding/Replacing a policy entry in an existing policy:

```
switch(config)# policy MY_POLICY
switch(config-policy)# 10 class ip MY_CLASS3 action drop action dscp af21
switch(config-policy)# exit
switch(config)# show policy
 Name
Sequence Comment
 Class Type
 action

 MY_POLICY
10
```

```

 MY_CLASS3 ipv4
 drop
 dscp AF21

20
 MY_CLASS3 ipv4
 mirror 1

```

Removing a policy entry:

```

switch(config)# policy MY_POLICY
switch(config-policy)# no 10
switch(config-policy)# exit
switch(config)# show policy
 Name
 Sequence Comment
 Class Type

 MY_POLICY
20
 MY_CLASS3 ipv4
 mirror 1

```

Removing a policy:

```

switch(config)# no policy MY_POLICY
switch(config)# show policy
Name Sequence Comment Class Type action

MY_POLICY 22 MY_CLASS3 ipv4 mirror 1

```

The policer **exceed** DSCP action cannot be combined with other actions in the same policy entry, but other entries in the policy may use other actions.

For example, this configuration is valid:

```

switch(config)# policy my_policy
switch(config-policy)# 10 class ip my_class action cir kbps 1000 cbs 15625 exceed
dscp EF

```

But this is not because it adds a secondary action within the same policy entry:

```

6300(config-policy)# 10 class ip my_class action cir kbps 1000 cbs 15625 exceed
dscp EF action mirror 1

```

Invalid input: action



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                                                                                      | Authority                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code><br>The <b>policy</b> command takes you into the <b>config-policy</b> context where you enter the policy entries. | Administrators or local user group members with execution rights for this command. |

## policy copy

`policy <POLICY-NAME> copy <DESTINATION-POLICY>`

### Description

Copies a policy to a new destination policy or overwrites an existing policy. Copying a policy copies all its entries as well.

| Parameter                               | Description                                   |
|-----------------------------------------|-----------------------------------------------|
| <code>&lt;POLICY-NAME&gt;</code>        | Specifies the policy to be copied.            |
| <code>&lt;DESTINATION-POLICY&gt;</code> | Specifies the name of the destination policy. |

### Examples

Copying a policy:

```
switch(config)# policy MY_POLICY copy MY_POLICY2
switch(config)# do show policy
 Name
Sequence Comment
Class Type
 action

 MY_POLICY
 2
 my_class3 ipv4
 mirror 1

 MY_POLICY2
 2
 my_class3 ipv4
 mirror 1
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## policy resequence

policy <POLICY-NAME> resequence <STARTING-SEQ-NUM> <INCREMENT>

### Description

Resequences numbering in a policy.

| Parameter          | Description                                                       |
|--------------------|-------------------------------------------------------------------|
| <POLICY-NAME>      | Specifies the policy where you want to resequence policy entries. |
| <STARTING-SEQ-NUM> | Specifies the sequence number to start resequencing from.         |
| <INCREMENT>        | Specifies how much to increment the sequence numbers by.          |

### Examples

Resequencing a policy:

```
switch(config)# policy MY_POLICY resequence 1 1
switch(config)# do show policy
 Name
Sequence Comment
 Class Type
 action

 MY_POLICY
1 MY_CLASS3 ipv4
 drop
 dscp AF21

2 MY_CLASS3 ipv4
 mirror 1
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## policy reset

`policy <POLICY-NAME> reset`

### Description

Changes the user-specified policy configuration to match the active policy configuration. Use this command when a discrepancy exists between what the user configured and what is active and accepted by the system.

| Parameter     | Description                       |
|---------------|-----------------------------------|
| <POLICY-NAME> | Specifies the policy to be reset. |

### Examples

Resetting a policy:

```
switch(config)# policy MY_POLICY reset
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show class

`show class [ip | ipv6 | mac] [<CLASS-NAME>] [commands] [configuration] [vsx-peer]`

## Description

Shows class configuration information.

All parameters are optional.

| Parameter         | Description                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ip   ipv6   mac] | Selects the class type for the display: <b>ip</b> for IPv4, <b>ipv6</b> for IPv6, or <b>mac</b> for MAC classes.                                                                                                                                                                                              |
| <CLASS-NAME>      | Specifies the class name.                                                                                                                                                                                                                                                                                     |
| commands          | Specifies whether to display output as the CLI commands showing the configured class entries.                                                                                                                                                                                                                 |
| configuration     | Specifies whether to display classes that have been configured by the user, even if they are not active due to issues with the command parameters or hardware issues. This parameter is useful during a mismatch between the entered configuration and the previous successfully programmed (active) classes. |
| vsx-peer          | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                                                              |

## Examples

Showing all class configuration:

```
switch# show class
Type Name
 Sequence Comment
 action L3 Protocol
 Source IP address Source L4 Port(s)
 Destination IP address Destination L4 Port(s)
 Additional Parameters

ipv4 MY_IPV4_CLASS
 10 my first class entry comment
 match icmp
 192.168.0.1/255.255.255.0
 192.168.1.1/255.255.255.0
 VLAN: 1
 20 my second class entry comment
 ignore tcp
 10.100.0.10/255.255.255.0 < 3000
 10.100.1.10/255.255.255.0 > 2000
 VLAN: 1

```

Showing class configuration for the IPv4 class MY\_IPV4\_CLASS as CLI commands:

```
switch# show class ip MY_IPV4_CLASS commands
class ip "MY_IPV4_CLASS"
 10 match icmp 192.168.0.1/255.255.255.0 192.168.1.1/255.255.255.0 vlan 1
 10 comment my first class entry comment
 20 ignore tcp 10.100.0.10/255.255.255.0 lt 3000 10.100.1.10/255.255.255.0 gt
```



```
2000 vlan 1
20 comment my second class entry comment
```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show policy

Syntax that shows information for all policies:

```
show policy [commands] [configuration] [vsx-peer]
```

Syntax that filters by policies applied to an interface or VLAN:

```
show policy [interface <IF-NAME> [in | out | routed-in] | vlan <VLAN-ID> [in] | vni <VNI-ID> [routed-in]]
[commands] [configuration] [vsx-peer]
```

Syntax that filters by the named policy:

```
show policy <POLICY-NAME> [commands] [configuration] [vsx-peer]
```

Syntax that filters by the globally applied policy:

```
show policy global [commands] [configuration] [vsx-peer]
```

Syntax that shows statistical information in the form of hit counts:

```
show policy hitcounts <POLICY-NAME> [interface <IF-NAME> [in | routed-in] |
vlan <VLAN-ID> [in] | vni <VNI-ID> [routed-in]] [vsx-peer]
```

Syntax that shows statistical information in the form of hit counts for the globally applied policy:

```
show policy hitcounts global [vsx-peer]
```

## Description

Shows information about your defined policies and where they have been applied. When **show policy** is entered without parameters, information for all policies is shown. The parameters filter the list of policies for which information is shown.

Available filtering includes:

- The content of a specific policy.
- All policies applied to a specific interface.
- All policies applied to a specific VLAN.

- All policies applied to a specific VNI.
- The globally applied policy.

To display policy statistics, use the **show policy hitcounts** form of this command.



When a policy is applied to a physical interface or lag using command **apply policy**, with the **per-interface** parameter included, unique instances of the policy are applied to each physical interface port or LAG. The unique instance of a policy has a parent-child relationship with the policy from which it was created. The **show policy** command shows information about the parent policy not the unique instances.



If a policy contains any class entries with the count keyword and policy entries with the **cir** action, and the policy is applied to multiple physical or virtual interfaces in the same direction, except for the routed ingress direction, the statistics will be aggregated. In the routed ingress direction, the statistics will be aggregated in multiple physical or virtual interfaces in the same VRF. If separate statistics for different physical or virtual interfaces are required, then another policy should be created. Alternatively, in the case of physical interfaces or LAGs, a policy applied with **per-interface** set can be used.

| Parameter                              | Description                                                                                                                                                                                                                                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>interface &lt;IF-NAME&gt;</code> | Specifies the interface name.                                                                                                                                                                                                                                                                                        |
| <code>vlan &lt;VLAN-ID&gt;</code>      | Specifies the VLAN.                                                                                                                                                                                                                                                                                                  |
| <code>vni&lt;VNI-ID&gt;</code>         | Specifies the VNI.                                                                                                                                                                                                                                                                                                   |
| <code>in</code>                        | Selects the inbound (ingress) traffic direction.                                                                                                                                                                                                                                                                     |
| <code>routed-in</code>                 | Selects the routed in traffic direction. Not applicable to a policy applied to a VLAN.                                                                                                                                                                                                                               |
| <code>&lt;POLICY-NAME&gt;</code>       | Specifies the policy name.                                                                                                                                                                                                                                                                                           |
| <code>commands</code>                  | Causes the policy definition to be shown as the commands and parameters used to create it rather than in tabular form.                                                                                                                                                                                               |
| <code>configuration</code>             | Causes the user-configured policies be shown as entered, even if the policies are not active due to policy-definition command issues or hardware issues. This parameter is useful if there is a mismatch between the entered configuration and the previous successfully programmed (active) policies configuration. |
| <code>global</code>                    | Selects the globally applied policy.                                                                                                                                                                                                                                                                                 |
| <code>hitcounts</code>                 | Selects the policy hit counts (statistics). The switch displays the number of accepted bytes/conformed bytes (green and yellow bytes) as 0 kbps.                                                                                                                                                                     |
| <code>vsx-peer</code>                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                                                                     |

## Examples

Showing information for all policies:

```

switch# show policy
 Name
Sequence Comment
 Class Type
 action

 my_policy
10 QOS class
 class1 ipv4
 dscp af21
 drop
20 PBR policy.
 class2 ipv4
 pbr mypbr

```

Showing a policy as commands:

```

switch# show policy commands
policy my_policy
 10 class ip class1 action dscp af21 action drop
 20 class ip class2 action pbr mypbr

```

Showing the globally applied policy:

```

switch# show policy global commands
policy global1
 10 class ip my_class1 action drop
apply policy my_policy in

```

Showing policy hit counts (statistics) for the globally applied policy: :

```

switch# show policy hitcounts global
Statistics for Policy My_Policy:
global (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

```

Showing policy hit counts (statistics) for a policy applied everywhere (with 1/1/1 and 1/1/5 being applied per interface):

```

switch# show policy hitcounts My_Policy
Statistics for Policy My_Policy:

Interface 1/1/1,lag1 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any

```

```

 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 - 10 match tcp any any ack
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

Interface 1/1/4 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

Interface 1/1/5 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

interface 1/1/2.10,1/1/3.10 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 - 10 match tcp any any ack
 0 20 match icmpv6 1000::10 any count [0 kbps conform]
...
Statistics for Policy My_Policy:

Interface 1/1/1,lag1 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 - 10 match tcp any any ack
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

Interface 1/1/4 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

Interface 1/1/5 (in):
 Matched Packets Configuration
10 class ip My_ip_Class

```

```

0 10 match tcp any any ack count
- 20 match udp any lt 8 any
0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
0 10 match tcp any any count [0 kbps conform]
0 20 match icmpv6 1000::10 any count [0 kbps conform]

interface 1/1/2.10,1/1/3.10 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 - 10 match tcp any any ack
 0 20 match icmpv6 1000::10 any count [0 kbps conform]
...

```

Showing policy hit counts (statistics) for a policy applied on physical interfaces and LAGs:

```

switch# show policy hitcounts My_Policy interface 1/1/1
Statistics for Policy My_Policy:

Interface 1/1/1,lag1 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

```

Showing policy hit counts (statistics) for a policy applied on VLANs:

```

switch# show policy hitcounts My_Policy vlan 30
Statistics for Policy My_Policy:

vlan 30 (in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

```

Showing policy hit counts (statistics) for a policy applied on interface VLANs:

```

switch# show policy hitcounts My_Policy interface vlan10
Statistics for Policy My_Policy:

VRF red
interface vlan 10 (routed-in):
 Matched Packets Configuration
10 class ip My_ip_Class

```

```

0 10 match tcp any any ack count
- 20 match udp any lt 8 any
0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
0 10 match tcp any any count [0 kbps conform]
0 20 match icmpv6 1000::10 any count [0 kbps conform]

```

Showing policy hit counts (statistics) for a policy applied on interface VLANs for a specific VRF:

```

switch# show policy hitcounts My_Policy vrf red routed-in
Statistics for Policy My_Policy:

VRF red
interface vlan 10 (routed-in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]
Statistics for Policy My_Policy:

VRF red
interface vlan 10 (routed-in):
 Matched Packets Configuration
10 class ip My_ip_Class
 0 10 match tcp any any ack count
 - 20 match udp any lt 8 any
 0 30 match icmp any 10.1.1.10 count
20 class ipv6 My_ipv6_Class action cir kbps 1000000 cbs 1000000 exceed drop
 0 10 match tcp any any count [0 kbps conform]
 0 20 match icmpv6 1000::10 any count [0 kbps conform]

```



For more information on features that use this command, refer to the ACLs and Classifier Policies Guide for your switch model.

## Command History

| Release          | Modification                                                |
|------------------|-------------------------------------------------------------|
| 10.08            | Added <b>[per-interface]</b> information. Updated examples. |
| 10.07 or earlier | --                                                          |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## alias

```
alias <ALIAS-NAME> <COMMAND-STRING>
no alias <ALIAS-NAME><COMMAND-STRING>
```

### Description

Defines an alias for one or more CLI commands. The alias and its definition are valid only for the user that creates the alias.



The alias name cannot be an existing token name.

The **no** form of this command removes the specified alias.

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ALIAS-NAME>     | Specifies the name of the alias you are defining.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <COMMAND-STRING> | Specifies one or more commands and their parameters. Separate commands with a semicolon (;). Length: 1 to 400 characters. For commands that require user-supplied parameters, use <b>\$1</b> through <b>\$n</b> , in order, as placeholders. These parameters are replaced by the corresponding arguments from the command line, and must match the number of parameters required by the original command. For alias definitions that include multiple commands, continue numbering parameters through all commands. Do not restart numbering for each command. |

### Examples

Defining an alias:

```
switch(config)# alias srci show running-config interface $1
switch(config)# srci?
shv Execute "show alias" to list the command list. Arguments to replace $1,
 $2 etc.
switch(config)# show alias
Alias Name Alias Definition

srci show running-config interface $1
```

Using **alias** in config context:

```
switch(config)# srci 1/1/1
interface 1/1/1
no shutdown
```

```
ip address 1.1.1.1/24
exit
```

Using **alias** in enable context:

```
switch# srci 1/1/1
interface 1/1/1
 no shutdown
 ip address 1.1.1.1/24
exit
```

Using **alias** in operator context:

```
switch> srci 1/1/1
interface 1/1/1
 no shutdown
 ip address 1.1.1.1/24
exit
```

Removing an alias:

```
switch(config)# no alias srci show running-config interface $1
switch(config)# show alias
Alias Name Alias Definition

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## auto-confirm

```
auto-confirm
no auto-confirm
```

### Description

Specifies that the CLI automatically enters the affirmative response (**y**) to all confirmation prompts, enabling commands to execute without waiting for user confirmation.

The **no** form of this command sets auto-confirmation to the default value disabled.

### Usage



Some commands, such as **boot** command, prompt to confirm execution of the command or to save the current configuration. Typically, such commands display a confirmation message similar to the following:

```
Continue (y/n)?
```

This command is useful for automating switch configuration, but Hewlett Packard Enterprise recommends that you use the REST API instead of using CLI scripts to automate configuration operations.

When the switch reboots, auto-confirmation is set to the default (disabled).

## Example

```
switch# auto-confirm
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# configure terminal

```
configure [terminal]
```

## Description

Enters the global configuration (**config**) context.

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| terminal  | Configure from the terminal. This is the default parameter. |

## Example

```
switch# configure terminal
switch(config)#
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## disable

disable

### Description

Exits the manager context (#) and enters the operator context (>).

### Example

```
switch# disable
switch>
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## do

do <COMMAND>

### Description

Executes a manager context (#) or operator context (>) command from a configuration (**config**) context.



You can execute **exec** commands from a configuration context with or without using the **do** command.

| Parameter | Description                                                                       |
|-----------|-----------------------------------------------------------------------------------|
| <COMMAND> | Specifies the manager context (#) or the operator context (>) command to execute. |

### Usage

You can execute **exec** commands from a configuration context with or without using the **do** command.

Use the **do** command to execute commands such as **clear**, **checkpoint**, **auto-confirm** and **show** commands while you are in a configuration context (such as **config** or **config-vlan-10**).

For all **exec** commands you can use with the **do** command, from the global configuration context (**config**), enter **do**, followed by a space, and then press the tab key twice.

## Examples

Clearing LLDP neighbors from the global configuration context:

```
switch(config)# clear lldp neighbors
switch(config)# do clear lldp neighbors
switch(config)#
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                                    | Authority                                                                          |
|---------------|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | A configuration context such as <code>config</code> or <code>config-vlan-10</code> | Administrators or local user group members with execution rights for this command. |

# enable (manager context)

enable

## Description

Exits the operator context (>) and enters the manager context (#).

## Example

```
switch> enable
switch#
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Operator (>)    | Administrators or local user group members with execution rights for this command. |

# end

end

## Description

Exits the current context and enters the manager context (#).

## Example

```
switch# configure terminal
switch(config)# vlan 10
switch(config-vlan-10)# vlan 22
switch(config-vlan-22)# end
switch#
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Any context     | Administrators or local user group members with execution rights for this command. |

# exit

exit

## Description

Exits the current context and enters its parent context.

## Example

```
switch# configure terminal
switch(config)# vlan 10
switch(config-vlan-10)# vlan 22
switch(config-vlan-22)# exit
switch(config)# exit
switch#
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Any context     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## list

list

### Description

Shows a list of commands available from the current context.

### Example

```
switch> list
list
enable
exit
show session-timeout
...
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Any context     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## logout

logout

### Description

Terminates the current CLI session. Only an admin user will be prompted to save configuration before logging out. If saving the configuration fails then the logout operation is aborted.

For a non-admin user the session is terminated without saving the configuration similar to the **exit** command.

### Examples

Logging out and saving the configuration:

```
switch# logout
Do you want to save the current configuration (y/n)? y
The running-config is saved to startup-config. Logging out...

(C) Copyright 2017-2025 Hewlett Packard Enterprise Development LP

RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use, or copying. License found at
https://www.hpe.com/software/SW Licensing.
By using the software, you acknowledge that you have read and understand
the license, represent you are authorized to accept this license, and agree
to be bound by its terms. If you do not agree to these terms, do not use the
software. Consistent with FAR 12.211 and 12.212, Commercial Computer Software,
Computer Software Documentation, and Technical Data for Commercial Items are
licensed to the U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:
 * Software feature updates
 * New product announcements
 * Special events
Please register your products now at: https://networkingsupport.hpe.com

switch login:
```

Logging out without saving the configuration:

```
switch# logout
Do you want to save the current configuration (y/n)? n
Logging out without saving configuration...

(C) Copyright 2017-2025 Hewlett Packard Enterprise Development LP

RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use, or copying. License found at
https://www.hpe.com/software/SW Licensing.
By using the software, you acknowledge that you have read and understand
the license, represent you are authorized to accept this license, and agree
to be bound by its terms. If you do not agree to these terms, do not use the
software. Consistent with FAR 12.211 and 12.212, Commercial Computer Software,
Computer Software Documentation, and Technical Data for Commercial Items are
licensed to the U.S. Government under vendor's standard commercial license.

We'd like to keep you up to date about:
 * Software feature updates
 * New product announcements
 * Special events
Please register your products now at: https://networkingsupport.hpe.com

switch login:
```

When saving the configuration fails:

```
switch# logout
Do you want to save the current configuration (y/n)? y
The running-config could not be saved to the startup-config.
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Any context     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## page

page [<LINES>]  
no page

### Description

Specifies the number of output lines the CLI displays before pausing to wait for a user to press a key. This value is the number of lines supported by the terminal session. This setting is not persistent and applies to the current session only.

The **page** command is enabled by default on the switch with the number of lines supported by the terminal. Change this default by using the **page** command to specify a different number of output lines.

The **no** form of this command sets the number of lines that are displayed to the default, which is the number of lines supported by the current terminal session.

| Parameter | Description                                                                                                                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LINES>   | Specifies the number to display before pausing. If not specified, the number of lines supported by the current terminal session is used. Range: 2-1000 lines.<br>Default: The number of lines supported by the current terminal session |

### Examples

Setting the page size to an unlimited number of lines:

```
switch# no page
switch#
```

Example output of a command after setting the page size to 10 lines:

```
switch# page 10
switch# list
 show hostname
 show domain-name
list
configure { terminal }
```

```

disable
exit
end
page
page <2-1000>
-- MORE --, next page: Space, next line: Enter, quit: q

```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## Pipe (|) command

```

show running-config | begin 2 "vlan" | redirect "abc.txt"
show running-config | include "vlan" | exclude "vlan2" | count
show vlan | include "up" | include "VLAN100"

```

```
list | include "show" | exclude "show" | count
```

## Description

The pipe (|) command filters the output of **show** or **list** commands using the options **include**, **exclude**, **begin**, **count**, or **redirect**.

## Usage

```

show {<SHOW-COMMAND-OPTIONS>}... [| {include <PATTERN-STRING> |
 exclude <PATTERN-STRING> |
 begin {<LINES-TO-DISPLAY>} <PATTERN-STRING>}}...
 [| {count [<PATTERN-STRING>] |
 redirect [<FILE-NAME>}}]

```

```

list [| {include <PATTERN-STRING> |
 exclude <PATTERN-STRING> |
 begin {<LINES-TO-DISPLAY>} <PATTERN-STRING>}}...
 [| {count [<PATTERN-STRING>] |
 redirect [<FILE-NAME>}}]

```

- The pipe (|) command is supported for use with the **show** and **list** commands only.
- You can use multiple pipe commands with a single **show** or **list** command.

## Examples

```

show running-config | redirect "abc.txt"
show running-config | begin 2 "vlan" | begin -2 "vlan" | begin "vlan"
show running-config | include "vlan" | exclude "vlan2" | count
show vlan | include "up" | include "VLAN100"
list | include "show" | exclude "show" | count

```



## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## repeat

repeat [id <POSITION>] [<COUNT>] [<DELAY>]

### Description

Repeatedly executes one or more commands. By default, the most recent command in the history is executed until you press Ctrl+C.

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POSITION> | Specifies the position of a command, or range of positions of multiple commands, in the history list as shown in the output of the <b>show history</b> command. <POSITION> can be a single number, a comma-separated list of numbers, or a range of numbers specified by the beginning and end of the range, separated by a hyphen.<br>If the <b>id</b> parameter is not specified, the <b>repeat</b> command executes the command that was entered most recently. Default: 1. |
| <COUNT>    | Specifies number of times to execute the command or commands. Default: The command repeats an infinite number of times.                                                                                                                                                                                                                                                                                                                                                        |
| <DELAY>    | Specifies the number of seconds to delay before executing the command. Default: 2                                                                                                                                                                                                                                                                                                                                                                                              |

### Example

```
switch# repeat id 1-4,7-8,10 count 2 delay 3
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## session-timeout

```
session-timeout <MINUTES>
no session-timeout <MINUTES>
```

### Description

Specifies the number of minutes a CLI session can be idle before the session is automatically terminated and the user is logged out.

The **no** form of this command sets the timeout to the default value of 30 minutes.

| Parameter | Description                                                                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MINUTES> | Specifies the number of minutes the CLI session can remain idle. Specify 0 to configure CLI sessions to never time out. Range: 0 to 4320. Default: 30 |

### Example

```
switch(config)# session-timeout 15
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show session-timeout

```
show session-timeout [vsx-peer]
```

### Description

Shows the configured session timeout value.

| Parameter | Description                                                       |
|-----------|-------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not |

| Parameter | Description                                                                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

```
switch# show session-timeout
session-timeout: 30 minutes (Default)
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show alias

show alias [vsx-peer]

## Description

Shows the command aliases that are defined on the switch.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

```
switch# show alias
Alias Name Alias Definition

hst hostname int_config interface $1; no shutdown; ip address
$2; lldp receive; mtu $3; exit

switch# show hst
Alias Name Alias Definition

hst hostname
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show history

`show history [all-sessions] [timestamp]`

### Description

Shows all commands that have been executed by the user in the current session. Up to 500 commands executed by the user in the current session will be displayed.

| Parameter                 | Description                                                                                     |
|---------------------------|-------------------------------------------------------------------------------------------------|
| <code>all-sessions</code> | Specifies that the output includes commands from previous sessions. Limit 1000.                 |
| <code>timestamp</code>    | Specifies that the output include the time of execution of each command in the command history. |



If you specify the `all-sessions` and `timestamp` parameters in the same command, **timestamp** must always be entered after **all-sessions**. It cannot come before.

### Example

Showing a list of commands executed during the current CLI session:

```
switch# show history
12 start-shell
11 platform forwarding-table-mode 4
10 show running-config
9 configure
8 session-timeout 0
7 exit
6 boot set-default primary
5 show feature-pack
4 show logging
3 show int mgmt
2 show version
1 configure
```

Showing a list of commands executed during the current CLI session with timestamps:

```

switch# show history timestamp
12 Fri Mar 9 12:35:54 2018 start-shell
11 Fri Nov 10 05:19:00 2023 platform forwarding-table-mode 4
10 Fri Nov 10 05:19:00 2023 show running-config
9 Fri Nov 10 05:19:00 2023 configure
8 Fri Nov 10 05:19:00 2023 session-timeout 0
7 Fri Nov 10 05:19:07 2023 exit
6 Fri Nov 10 05:19:13 2023 boot set-default primary
5 Fri Nov 10 05:19:13 2023 show feature-pack
4 Fri Nov 10 05:19:13 2023 show logging
3 Fri Nov 10 05:29:50 2023 show int mgmt
2 Fri Nov 10 05:44:23 2023 show version
1 Fri Nov 10 07:47:55 2023 configure

```

Showing a list of commands executed by the user in the current session and during all previous CLI sessions:

```

switch# show history all-sessions
13 start-shell
12 platform forwarding-table-mode 4
11 show running-config
10 configure
9 session-timeout 0
8 exit
7 boot set-default primary
6 show feature-pack
5 show logging
4 show int mgmt
3 show version
2 configure
1 exit

```

Showing a list of commands executed by the user in the current session and during all previous sessions with timestamps:

```

switch# show history all-sessions timestamp
13 Fri Mar 9 12:35:54 2018 start-shell
12 Fri Nov 10 05:19:00 2023 platform forwarding-table-mode 4
11 Fri Nov 10 05:19:00 2023 show running-config
10 Fri Nov 10 05:19:00 2023 configure
9 Fri Nov 10 05:19:00 2023 session-timeout 0
8 Fri Nov 10 05:19:07 2023 exit
7 Fri Nov 10 05:19:13 2023 boot set-default primary
6 Fri Nov 10 05:19:13 2023 show feature-pack
5 Fri Nov 10 05:19:13 2023 show logging
4 Fri Nov 10 05:29:50 2023 show int mgmt
3 Fri Nov 10 05:44:23 2023 show version
2 Fri Nov 10 07:47:55 2023 configure
1 Fri Nov 10 08:02:11 2023 exit

```

Attempting to specify the timestamp parameter before the all-sessions parameter:

```

switch# show history timestamp all-sessions
Invalid input: all-sessions

```

## Command History

| Release          | Modification        |
|------------------|---------------------|
| 10.14            | All-sessions added. |
| 10.07 or earlier | --                  |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### cli-session

```
cli-session
no cli-session
```

#### Description

Enters the CLI session context (shown in the switch prompt as **config-cli-session**) for the purpose of configuring CLI user session management. Session management enhances security by enforcing specific CLI user session requirements. The following information is provided at time of successful login:

- When applicable, the number of failed login attempts since the most recent successful login.
- The date, time, and location (console or IP address or hostname) of the most recent previous successful login.
- The count of successful logins within the past (configurable) time period.

For example:

```
switch login: admin
Password:
```

```
There were 3 failed login attempts since the last successful login
Last login: 2019-04-20 08:51:33 from the console
User "admin" has logged in 73 times in the past 30 days
```

The no form of this command disables concurrent CLI user session restrictions and reverts **timeout** and **tracking-range** to their default values.



---

To ensure that enhanced security is maintained, it is recommended that you keep CLI user session management fully enabled by setting **max-per-user** to a nondefault value.

---



---

The **cli-session** command applies only to SSH/console login connection types. It does not apply to other connection types such as REST.

---

#### Subcommands

These subcommands are available within the CLI session context.

```
[no] max-per-user <SESSIONS>
```

Specifies the maximum number of concurrent CLI sessions per user. The no form of this subcommand disables concurrent CLI user session restrictions. Default: Disabled (no value). Range: 1 to 5.



When the same user name is configured for both local and remote authentication, both users, regardless of privilege level, are considered to be the same user for the purpose of counting concurrent CLI sessions. For example, with **max-per-user** set to 1 and user **admin1** configured for local and remote authentication, only the local user **admin1** or the remote user **admin1** can be logged in at any given moment. Both **admin1** users cannot be logged in simultaneously unless **max-per-user** is increased to at least 2.

[no] **timeout** <MINUTES>

Specifies the number of minutes a CLI session can be idle before the session is automatically terminated and the user is logged out. A value of 0 minutes disables the session timeout. The no form of this subcommand sets the timeout value to the default. Default 30: Range 0 to 4320.



This subcommand is the recommended replacement for the **session-timeout** command.

[no] **tracking-range** <DAYS>

Specifies the maximum number of days to track CLI user session logins. The no form of this subcommand resets the value to its default. Default 30: Range 1 to 30.

**exit**

Exits the CLI session context.

**end**

Exits the CLI session context and then the config context.

## Examples

Configuring CLI user session settings for a maximum of one concurrent session, a 20-minute timeout, and tracking for a maximum of 25 days.

```
switch(config)# cli-session
switch(config-cli-session)# max-per-user 1
switch(config-cli-session)# timeout 20
switch(config-cli-session)# tracking-range 25
switch# exit
```

After successful earlier logins, logging in from the console without any intervening unsuccessful logins.

```
switch login: admin1
Password:

Last login: 2019-04-15 14:10:21 from the console
User 'admin1' has logged in 65 times in the past 25 days
```

Attempting to log in as **admin1** when already logged in as **admin1** from elsewhere.

```
switch login: admin1
Password:
Too many logins for 'admin1'
```

After successful earlier logins, attempting to log in twice with an invalid password, followed by a successful login.

```
switch login: admin1
Password:
```



```
Login incorrect
switch login: admin1
Password:

Login incorrect
switch login: admin1
Password:

There were 2 failed login attempts since the last successful login
Last login: 2019-04-15 17:22:45 from 192.168.1.1
User 'admin1' has logged in 72 times in the past 25 days
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## clock date

clock date <DATE>

### Description

Sets the switch date.

| Parameter | Description                                     |
|-----------|-------------------------------------------------|
| <DATE>    | Specifies the date. Format: <b>YYYY-MM-DD</b> . |

### Examples

This example sets the date to Dec 14, 2017.

```
switch(config)# clock date 2017-12-14
```

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## clock datetime

clock datetime <DATE> <TIME>

### Description

Sets the switch date and time.

| Parameter | Description                                     |
|-----------|-------------------------------------------------|
| <DATE>    | Specifies the date. Format: <b>YYYY-MM-DD</b> . |

| Parameter | Description                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------------------|
| <TIME>    | Specifies the time in 24-hour clock format. Seconds are optional. Format: <b>HH:MM</b> or <b>HH:MM:SS</b> . |

## Examples

This example sets the date and time to Dec 13, 2017 at 15:00.

```
switch(config)# clock datetime 2017-12-13 14:15:00
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# clock time

clock time <TIME>

## Description

Sets the switch time.

| Parameter | Description                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------------------|
| <TIME>    | Specifies the time in 24-hour clock format. Seconds are optional. Format: <b>HH:MM</b> or <b>HH:MM:SS</b> . |

## Examples

This example sets the time to 15:01:23.

```
switch(config)# clock time 15:01:23
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## clock timezone

```
clock timezone <TIME-ZONE>
no clock timezone [<TIME-ZONE>]
```

### Description

Sets the time zone and its associated daylight savings time rule.  
The **no** form of this command sets the time zone to the default value of UTC.

| Parameter   | Description                                                                                                                                                                                                                              |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <TIME-ZONE> | Specifies the time zone, <TIME-ZONE>, using a name defined in the IANA time zone database. See <a href="https://en.wikipedia.org/wiki/List_of_tz_database_time_zones">https://en.wikipedia.org/wiki/List_of_tz_database_time_zones</a> . |

### Examples

Setting the time zone to Eastern Standard Time (EST):

```
switch(config)# clock timezone EST
```

### Command History

| Release          | Modification                                                           |
|------------------|------------------------------------------------------------------------|
| 10.08            | Added optional <TIME-ZONE> parameter to <b>no</b> form of the command. |
| 10.07 or earlier | --                                                                     |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show clock

```
show clock
```

### Description

This command displays the current date, time, and time zone.

### Example

```
switch# show clock
Wed Nov 22 23:29:10 PDT 2017
System is configured for timezone : US/Pacific
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## Container management commands

### container

```
container <CONTAINER-NAME>
no container <CONTAINER-NAME>
```

#### Description

Enters into the container configuration context.

The **no** form of this command removes the existing configurations of the specified container.

| Parameter        | Description                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------|
| <CONTAINER-NAME> | The container name can contain up to 64 characters. Only letters, numbers and underscore ( _ ) characters are permitted. |

#### Example

Configures a new container:

```
switch(config)# container app
The feature being used requires a AOS-CX Advanced Software Feature Pack.
For more information, refer to the AOS-CX Feature Pack Deployment Guide.
```

AOS-CX does not enforce the requirement to own a feature pack prior to using container features. This warning message is displayed only during creation, subsequent calls to the container context will not display the message.



For more information on features that use this command, refer to the Containers guide for your switch model.

#### Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

#### Command Information

| Platforms | Command context                   | Authority                                                                          |
|-----------|-----------------------------------|------------------------------------------------------------------------------------|
| 9300      | config                            | Administrators or local user group members with execution rights for this command. |
| 9300S     | config-container-<CONTAINER-NAME> |                                                                                    |

# container exec

container <NAME> exec <PARAMS>

## Description

Allows the execution of an endpoint script in the container. The location of this endpoint is provided to the container manager infrastructure through a manifest file in the image file system of the container. This manifest file provides metadata related to the container application. When the exec command runs, the manifest information is used to determine the endpoint to execute and the user parameters are passed directly to the endpoint. The output of such execution is provided directly to the user through the CLI. In case the manifest information or the endpoint file are missing an error is presented to the user. The user can interrupt the execution by pressing **Ctrl+C**.



If the container is not operational when the command is executed, the following error message is returned:  
**Failed to execute endpoint - The container is not operational.**

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| <NAME>    | Specifies a container name up to 64 characters long. |
| exec      | Runs a container application command.                |
| <PARAMS>  | Specifies container command parameters.              |



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context                   | Authority                                                                          |
|---------------|-----------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container-<CONTAINER-NAME> | Administrators or local user group members with execution rights for this command. |

# enable

enable  
no enable

## Description

A container is disabled by default when it is created. Use the **enable** command to enable the container.

The **no** version of this command disables the container. When an enabled container is disabled, system resources are released but the container configuration settings are stored.

## Example

Enabling and then disabling the container **test**:

```
switch(config-container-test)# enable
switch(config-container-test)# no enable
```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release    | Modification       |
|------------|--------------------|
| 10.16.1000 | Command introduced |

## Command Information

| Platforms     | Command context                                 | Authority                                                                          |
|---------------|-------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container- <i>&lt;CONTAINER-NAME&gt;</i> | Administrators or local user group members with execution rights for this command. |

## env

```
env <NAME> {value <VALUE>}{encrypted [plaintext <VALUE>|ciphertext <VALUE>]}
no env <NAME> {value <VALUE>}{encrypted {plaintext|ciphertext}<VALUE>}
```

## Description

Configures an environment variable for a container that is composed of a key and a value pair. The key-value pair defines the behavior of the environment in a container and is used by the container processes. The value of the environment variable can be stored in the host system as an encrypted value. The container manager infrastructure provides the decrypted value to the container.

The **no** form of this command removes the configured environment variable from a container.



Configuring the **env** variable for an already operational container causes the container to restart if the container has already been enabled.

| Parameter                  | Description                                                                                                                       |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;NAME&gt;</i>        | Specifies the name of the container environment variables.                                                                        |
| <i>value &lt;VALUE&gt;</i> | Specifies the variable value.                                                                                                     |
| <i>encrypted</i>           | Encrypts the environment variable value. If you press <b>&lt;enter&gt;</b> after the <b>encrypted</b> parameter, you will enter a |



| Parameter                             | Description                                                                                                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | variable configuration mode that allows you to securely enter a hidden value. <i>This is the recommended method for entering an encrypted variable</i>                                     |
| <code>plaintext &lt;VALUE&gt;</code>  | <b>Optional.</b> Specifies the variable value in plain text. <i>Not recommended for encrypted variables.</i>                                                                               |
| <code>ciphertext &lt;VALUE&gt;</code> | <b>Optional.</b> Specifies the variable value as previously encrypted text. <i>Recommended for encrypted variables; specify the encrypted variable value as previously encrypted text.</i> |

## Example

Securely entering an encrypted variable:

```
6300(config-container-test)# env TEST encrypted
Enter environment variable value: *****
6300(config-container-test)# end
```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release    | Modification                                                                                                                                                                                                                                                     |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.13.1000 | The <b>plaintext</b> and <b>ciphertext</b> options for the encrypted parameter are now optional. Starting with this release, you can use the <b>encrypted</b> option to encrypt the environment variable and specify the value in plaintext hidden from the CLI. |
| 10.12      | Command introduced                                                                                                                                                                                                                                               |

## Command Information

| Platforms     | Command context                                      | Authority                                                                          |
|---------------|------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-container-&lt;CONTAINER-NAME&gt;</code> | Administrators or local user group members with execution rights for this command. |

## image-location

```
image-location <URL> vrf <VRF-NAME> [allow-unsigned]
no image-location <URL> <VRF-NAME> [allow-unsigned]
```

## Description

Configures the image location for a container. Modifying image location prompts an image upgrade. The **no** form of this command removes the configured location of a container.



- If the user sets a location value which does not follow the standard URL format, the following error message is returned: **Failure to configure image location: Invalid URL**
- If the user tries to use a VRF value that doesn't exist on the switch, the following error message is returned: **Failure to configure image location: Invalid VRF**
- If the image of the container exceeds the maximum image size supported by the switch, the container won't be deployed.

By default, only container images with a valid HPE signature are allowed. To bypass this signature check and allow unsigned container images, include the **allow-unsigned** parameter when you define the image location. The **allow-unsigned** parameter cannot be used if you have issued the **secure-mode enhanced** command to set the switch to enhanced secure mode.

| Parameter      | Description                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL            | Specifies the URL of the container application. URL supports HTTP protocol. The image-location URL can either be IPv4 or IPv6 address. The IPv6 address must be provided within square brackets. |
| vrf <VRF-NAME> | (Optional) Specifies the VRF of the image URL.                                                                                                                                                   |
| allow-unsigned | (Optional) Allow download and deployment of an unsigned container image.                                                                                                                         |

## Examples

Configures the image location for the IPv4 setting:

```
switch(config-container-1)# image-location http://10.0.0.1/container.img vrf mgmt
```

Appends the port to the address if the image server is running on a port other than HTTP for an IPv4 setting:

```
switch(config-container-1)# image-location http://10.0.0.1:9050/container.img vrf mgmt
```

Configures image location for IPv6 setting by wrapping IP address between square brackets:

```
switch(config-container-1)# image-location http://[2001::2]/container.img vrf mgmt
```

Specifies port number by appending it with the IPv6 address:

```
switch(config-container-1)# image-location http://[2001::2]:9050/container.img vrf mgmt
```

When you include the **allow-unsigned** parameter on a switch in standard secure mode, the following message will be displayed to inform this can be a potential security issue.

```
switch(config-container-1)# image-location http://10.0.0.1/container.img vrf mgmt
allow-unsigned
Allowing unsigned container images poses a potential security risk
that can impact both the current device and the entire network. By
allowing installation of unsigned applications you are acknowledging
and accepting these risks. HPE shall not be responsible for the
consequences of your actions and disclaims any and all liability.

Continue (y/n)? y
```

When you attempt to include the **allow-unsigned** parameter on a switch in enhanced secure mode, the following message will appear to indicate that this parameter is not supported.

```
switch(config-container-1)# image-location http://10.0.0.1/container.img vrf mgmt
allow-unsigned
Unsigned images are not permitted in the current secure mode, using the
allow-unsigned parameter will have no effect.
```

| Release | Modification                                       |
|---------|----------------------------------------------------|
| 10.14   | The <b>allow-unsigned</b> parameter is introduced. |
| 10.12   | Command introduced.                                |

## Command Information

| Platforms     | Command context                                 | Authority                                                                          |
|---------------|-------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container- <i>&lt;CONTAINER-NAME&gt;</i> | Administrators or local user group members with execution rights for this command. |

## mount

```
mount <id>
 destination <path>
 no ...
 source <TYPE> <PATH>
```

## Description

Mount persistent storage for a container application, and optionally indicate the mounted storage source and destination paths.

| Parameter                       | Description                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;ID&gt;</i>               | ID assigned to a mounted storage instance for a container application. Range: <1-4294967295>                                                                                                                      |
| destination <i>&lt;PATH&gt;</i> | The destination path is a directory or file inside the container file system. The path must use the syntax <b>/FILE DIRECTORY</b> . Only letters, numbers, slashes, underscores, dashes, and periods are allowed. |

| Parameter | Description                                                                                                                                                                                                                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| no ...    | Negates any configured parameter or removes a source or destination path.                                                                                                                                                                                                                                    |
| source    | Define the mounted storage source.                                                                                                                                                                                                                                                                           |
| <type>    | This version of AOS-CX supports only a <b>usb</b> storage type.<br><br><b>NOTE:</b> For containers using USB persistent storage functionality, <b>ext4</b> is the recommended formatting method for USB storage devices. While <b>FAT32</b> is currently supported, it may be deprecated in future releases. |
| <PATH>    | The mounted storage source path must be a valid file or directory on the USB device and is relative to the root directory of the device file system. The path must use the syntax <b>/ {FILE DIRECTORY}</b> . Only letters, numbers, slashes, underscores, dashes, and periods are allowed.                  |

## Example

Creating the mount ID 1 for the container **test**.

```
switch(config-container-test)# mount 1
```

Configuring container mount **1** with a **USB** source and the path **/app1-data**.

```
switch(config-container-mount-1)# source usb /app1-data
```

Configuring container mount **1** with the destination path **/app1-data**.

```
switch(config-container-mount-1)# destination /app1-data
```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release    | Modification       |
|------------|--------------------|
| 10.16.1000 | Command introduced |

## Command Information

| Platforms     | Command context                   | Authority                                                                          |
|---------------|-----------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container-<CONTAINER-NAME> | Administrators or local user group members with execution rights for this command. |

## network vrf

```
network vrf <VRF>
no network vrf <VRF>
```

## Description

Use this command to associate a VRF with the container and allow connectivity through the VRF. When configured, the VRF will be accessible to the container through a network namespace.

## Usage

Only one network VRF can be configured per container. If an additional VRF is configured, the container deployment will fail and generate an error message indicating that the container has more than one network VRF. Modifying a network container VRF will modify the container network configuration and the container will be restarted to apply the new changes if the container has already been enabled.

## Examples

The following example defines the VRF **mgmt** for the **app** container.

```
switch(config-container-app)# network vrf mgmt
```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context                                 | Authority                                                                          |
|---------------|-------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container- <i>&lt;CONTAINER-NAME&gt;</i> | Administrators or local user group members with execution rights for this command. |

## port-map

```
port-map host-port <PORT> container-port <PORT> protocol (tcp | udp)
```

## Description

Issue this command from the **config-container-network-vrf-*<name>*** context to define a port map from a port on the host switch to a port on the container. This will allow communication from external devices to services provided by the container.

| Parameter                          | Description                                 |
|------------------------------------|---------------------------------------------|
| host-port <i>&lt;port&gt;</i>      | The host switch port number. Range: 1-65535 |
| container-port <i>&lt;port&gt;</i> | The container port number. Range: 1-65535   |

| Parameter | Description                                      |
|-----------|--------------------------------------------------|
| tcp       | Communications will use the <b>TCP</b> protocol. |
| udp       | Communications will use the <b>UDP</b> protocol. |

## Usage

A port map is an optional configuration for a container network VRF, but a port mapping is required to expose the mapped port to the outside network. This command can be issued multiple times to define more than one port map for the container.



Host port conflicts are not allowed. The same host port cannot be used for different containers in the same VRF, and the host port used for the VRF cannot be reserved for a non-container application on the host switch.

## Examples

Configure a port map from the host to the container for TCP traffic, where traffic to TCP port 8000 on the switch will be directed to TCP port 9000 in the container.

```
switch(config-container-network-vrf-mgmt)# port-map host-port 8000 container-port 9000 protocol tcp
```

The following example maps different ports on the host to the same container port for TCP traffic:

```
switch(config-container-network-vrf-mgmt)# port-map host-port 8000 container-port 9000 protocol tcp
switch(config-container-network-vrf-mgmt)# port-map host-port 8001 container-port 9000 protocol tcp
```

The following example maps the same port on the host switch to the same container port for TCP and UDP traffic:

```
switch(config-container-network-vrf-mgmt)# port-map host-port 8000 container-port 9000 protocol tcp
switch(config-container-network-vrf-mgmt)# port-map host-port 8000 container-port 9000 protocol udp
```

The following example maps the same port on different VRFs on the host switch to the same container port for TCP traffic:

```
switch(config-container-network-vrf-mgmt)# port-map host-port 8000 container-port 9000 protocol tcp
switch(config-container-network-vrf-default)# port-map host-port 8000 container-port 9000 protocol tcp
```

When removing a port mapping, if the command parameters do not match a configured port mapping, the command output displays the following message:

```
switch(config-container-network-vrf-mgmt)# no port-map host-port 8001 container-
port 9000 protocol tcp
The specified port mapping is not configured
```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release    | Modification       |
|------------|--------------------|
| 10.16.1000 | Command introduced |

## Command Information

| Platforms     | Command context                   | Authority                                                                          |
|---------------|-----------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container-<CONTAINER-NAME> | Administrators or local user group members with execution rights for this command. |

## restrict cpu

```
restrict cpu <PERCENTAGE>
no restrict cpu
```

### Description

Configures limitations for the container CPU usage. The CPU constraint is set as a percentage of the total switch CPUs. One container or any combination of containers configured on a switch can use up to 20% of the total CPU capacity of the device.



Configuring the CPU constraint for an already operational container will cause the container to restart if the container has already been enabled.

The **no** form of this command removes restrictions on the CPU usage, and reverts back to the default limitation of 10%.

| Parameter    | Description                                                                 |
|--------------|-----------------------------------------------------------------------------|
| <PERCENTAGE> | Specifies percentage for the container CPU usage, The default value is 10%. |



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context                                 | Authority                                                                          |
|---------------|-------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container- <i>&lt;CONTAINER-NAME&gt;</i> | Administrators or local user group members with execution rights for this command. |

## restrict memory

```
restrict memory <MB>
no restrict memory
```

### Description

Configures limitations for memory usage of the container. The memory constraint is set in MB, and the maximum 20% of the capacity of the device can be configured for any combination of containers running on the switch. Configuring the memory constraint for an already operational container restarts the container if the container has already been enabled.

The **no** form of this command removes restrictions on the memory usage and reverts back to the default limitation of 256 MB.

| Parameter         | Description                                                            |
|-------------------|------------------------------------------------------------------------|
| <i>&lt;MB&gt;</i> | Specifies the maximum memory usage in MB. The default value is 256 MB. |



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context                                 | Authority                                                                          |
|---------------|-------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container- <i>&lt;CONTAINER-NAME&gt;</i> | Administrators or local user group members with execution rights for this command. |

## show container

```
show container [<CONTAINER-NAME>] [[isolated-network <name>]]
```

### Description

Shows the configuration and status information of the containers or container isolated networks running in the system. If the container name is not specified, the output of this displays information for



all containers. When a container name is specified, the output displays information specific to that container.

| Parameter                           | Description                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------|
| <code>&lt;CONTAINER-NAME&gt;</code> | Specifies the name of the container for which information needs to be displayed |

## Usage

The **Container status** field in the output of this command can display any of the following status values:

- **initializing**: Container initialization and configuration verification is in progress.
- **waiting**: Container is waiting for configuration prerequisites to be met.
- **configuration failed**: User-specified container configuration failed.
- **network configuration failed**: Container network provisioning failed.
- **acquiring**: Container is acquiring an image.
- **acquire failed**: Container failed to acquire an image.
- **deploying**: Container is deploying.
- **operational**: Container is operational (deployed and running).
- **deploy failed**: Container failed to deploy.
- **run failed**: Container failed while running.
- **exited**: Container completed its execution and exited.

## Examples

The following example shows information for a configured container with a network VRF with port mappings:

```
switch# show container
Container : appl
Container status : operational
Manifest status : success
Image status : verified
Image version : 1.0.0
Image location VRF : mgmt
Image location URL : http://30.0.0.2:8000/container.img
CPU limit : 10%
Memory limit : 512MB
Environment variables:
 PYP=/usr/bin/python3
Encrypted environment variables:
 encryptedVar1
 encryptedVar2
Vrf Networks:
 VRF name : default
 Port map :
 8080:80/tcp
 8080:8080/udp
```

The following example shows additional error messages:

```

switch# show container
Container : app
Container status : configuration failed
Config failure reason : Multiple definitions of environment variable PYP
Manifest status : error
Manifest status reason : 'exec' file not found in container
Image status : verified
Image version : 1.0.0
Image location VRF : mgmt
Image location URL : http://30.0.0.2:8000/container.img
CPU limit : 10%
Memory limit : 512 MB
VRFs : mgmt
Environment variables :
 PYP=/usr/bin/python3
Encrypted environment variables:
 PYP
 encryptedVar2

```

The following example shows a configured container without signature validation:

```

switch# show container appl
Container : appl
Container status : operational
Manifest status : success
Image status : allowed without signature
Image version : 1.0.0
Image location VRF : mgmt
Image location URL : http://30.0.0.2:8000/container.img
CPU limit : 10%
Memory limit : 512 MB
Environment variables:
 PYP=/usr/bin/python3
Encrypted environment variables:
 encryptedVar1
 encryptedVar2
VRF Networks:
 VRF name : default
 Port map :
 8080:80/tcp
 8080:8080/udp

```

The following example shows the output of the show containers command out when there are no configured containers:

```

switch# show container
No containers configured

```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show capacities containers

show capacities containers

### Description

Shows the maximum number of containerized applications that can be configured in the system.

### Examples

Shows maximum number of containerized applications that can be configured:

```
switch# show capacities containers
System Capacities: Filter CONTAINERS
Capacities Name Value

Maximum number of containerized applications configurable in the system 2
```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show capacities-status containers

show capacities-status containers

### Description

Reserved for future use.



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show running-config container

show running-config container

## Description

Shows the running configuration of all the containers.

| Parameter | Description                                                       |
|-----------|-------------------------------------------------------------------|
| container | Specifies that container running configuration must be displayed. |

## Examples

Shows the running configuration for the container:

```
container app1
 enable
 image-location http://30.0.0.2:8000/container.img vrf mgmt
 restrict cpu 10
 restrict memory 512
 network vrf mgmt
 port-map host-port 8000 container-port 9000 protocol tcp
 exit
 mount 1
 source usb /app1-data
 destination /app-data
 exit
 env PYP value /usr/bin/python3
 env encryptedVar1 encrypted ciphertext AQBapcmTCVdag
container app2
 enable
 image-location http://[2001::2]:8000/changeValidation_x86_t.img vrf mgmt allow-
unsigned
 restrict cpu 5
 restrict memory 256
 network vrf default
 port-map host-port 7819 container-port 7819 protocol udp
 exit
 mount 1
 source usb /app2-data1
```

```

 destination /app-data1
 exit
 mount 2
 source usb /app2-data2
 destination /app-data2
 exit
 env PYP value /usr/bin/python3
 env encryptedVar1 encrypted ciphertext AQBapcmTCVdag
 env encryptedVar2 encrypted ciphertext AQPY4V4v9UtDa==

```



For more information on features that use this command, refer to the Containers guide for your switch model.

## Command History

| Release    | Modification                                                                      |
|------------|-----------------------------------------------------------------------------------|
| 10.16.1000 | The output of this command includes mount and network VRF details, if configured. |
| 10.12      | Command introduced                                                                |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## vrf

vrf <VRF-NAME>

## Description

This command is deprecated. Use the [network vrf](#) command to define a VRF for a container.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.12   | Command introduced |

## Command Information

| Platforms     | Command context                   | Authority                                                                          |
|---------------|-----------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-container-<CONTAINER-NAME> | Administrators or local user group members with execution rights for this command. |

## Classes of traffic

The different classes of traffic that can be individually configured are:

*Applies to the HPE Aruba Networking 8320, 8325, 9300/9300S, 10000 Switch Series:*

- **acl-logging**: Access Control List logging packets.
- **arp-broadcast**: Address Resolution Protocol packets with a broadcast destination MAC address.
- **arp-unicast**: Address Resolution Protocol packets with a switch system destination MAC address.
- **bfd**: Bidirectional Forwarding Detection (BFD) packets with a destination IP address owned by the switch.
- **bgp-ipv4**: Border Gateway Protocol packets with a destination IPv4 address owned by the switch.
- **bgp-ipv6**: Border Gateway Protocol packets with a destination IPv6 address owned by the switch.
- **dhcp-ipv4**: Dynamic Host Configuration Protocol packets with a destination IPv4 address.
- **dhcp-ipv6**: Dynamic Host Configuration Protocol packets with a destination IPv6 address.
- **dss: 10000**
- **erps**: Ethernet Ring Protection Switching control packets with the destination MAC address 01:19:a7:00:00:XX, where XX can be any value.
- **flow-telemetry**: Packets received for flow telemetry such as IP Flow Information Export (IPFIX).



The **flow-telemetry** class is not supported for HPE Aruba Networking 8320, 8325, 9300, 9300S, Switch series.

- **hypertext**: Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) packets.
- **icmp-broadcast-ipv4**: Internet Control Message Protocol packets with a broadcast or multicast destination IPv4 address.
- **icmp-multicast-ipv6**: Internet Control Message Protocol packets with a well-known multicast destination IPv6 address.
- **icmp-unicast-ipv4**: Internet Control Message Protocol packets with a destination IPv4 address owned by the switch.
- **icmp-unicast-ipv6**: Internet Control Message Protocol packets with a destination IPv6 address owned by the switch.
- **ieee-8021x**: IEEE 802.1X protocol packets with EtherType 0x088E.



The **flow-telemetry** class is not supported for HPE Aruba Networking 8320 9300, 9300S, Switch series.

- **igmp**: Internet Group Management Protocol packets.

- **ip-exceptions:** Routable packets that would exceed the MTU for the egress interface, packets that trigger ICMP redirects, and packets with TTL/hop\_limit=1 that are discarded when routing through the switch.
- **ipfix:** Packets received for IPFIX (IP Flow Information Export).




---

The **ipfix** class is not supported for HPE Aruba Networking 8320, 9300, 9300S, 10000, Switch series.

---

- **ipsec:** Internet Protocol Security IPv4 or IPv6, unicast or configured multicast. All IPsec traffic received by the CPU will be regulated by the **ipsec** class regardless of the encapsulated protocol.
- **ipv4-options:** Unicast IPv4 packets including option headers.
- **ipv6-options:** Unicast IPv6 packets including option headers.
- **lACP:** Link Aggregation Control Protocol packets with the destination MAC address 01:80:c2:00:00:02.
- **lldp:** Link Layer Discovery Protocol packets with the destination MAC address 01:80:c2:00:00:0e.
- **loop-protect:** Loop Protection packets with the destination MAC address 09:00:09:09:13:a6.
- **mdns:** Multicast Domain Name System packets.




---

The **mdns** class is not supported for HPE Aruba Networking 8320 Switch series.

---

- **mirror-to-cpu:** Packets from mirroring session configured to deliver to the console.
- **mld:** Multicast Listener Discovery packets of type V1 or V2 with an IPv6 address of FF00::/8, FF02::16 or FF02::2.
- **mvrp:** Multiple VLAN Registration Protocol packets with the destination MAC address 01:80:c2:00:00:20 or 01:80:c2:00:00:21.
- **ntp:** Network Time Protocol packets with a destination IP address owned by the switch.
- **ospf-multicast-ipv4:** Open Shortest Path First packets with the multicast destination IPv4 address 224.0.0.5 or 224.0.0.6. The HPE Aruba Networking 8325 Switch series has VxLAN packets with VNI 0.
- **ospf-multicast-ipv6:** Open Shortest Path First packets with the multicast destination IPv6 address FF02::5 or FF02::6.
- **ospf-unicast-ipv4:** Open Shortest Path First packets with a destination IPv4 address owned by the switch.
- **ospf-unicast-ipv6:** Open Shortest Path First packets with a destination IPv6 address owned by the switch.
- **pim:** Protocol Independent Multicast packets with the destination IPv4 address 224.0.0.13 or IPv6 address FF02::D, or Multicast Source Discovery Protocol (MSDP) packets, or with a destination IP address owned by the switch. Also includes PIM packets received from a 6in6 tunnel.
- **secure-learn: 10000**




---

The **secure-learn** class is not supported for HPE Aruba Networking 8320, 8325, and 9300, 9300S, Switch series.

---

- **sflow:** Packet headers sampled by the switch that will be sent to the sFlow collector.
- **ssh:** Secure Shell (SSH) or Secure File Transfer Protocol (SFTP) packets. Dropping ssh packets will result in the connection to the CLI being lost.
- **stp:** Spanning Tree Protocol (STP) packets with the destination MAC address 01:80:c2:00:00:00 or Per-VLAN Spanning Tree (PVST) packets with the destination MAC address 01:00:0c:cc:cc:cd.
- **telnet:** Secure Telnet packets.

- **udld:** Unidirectional Link Detection packets with the destination MAC address 01:00:0c:cc:cc:cc or 00:e0:52:00:00:00, or Cisco Discovery Protocol packets with the destination MAC address 01:00:0c:cc:cc:cc.
- **unknown-multicast:** Packets with an unknown multicast destination IP address.
- **unresolved-ip-unicast:** Packets to be software forwarded by the management processor.
- **vrrp-ipv4:** Virtual Router Redundancy Protocol packets with the destination IPv4 address 224.0.0.18 or VSW-Keepalive.
- **vrrp-ipv6:** Virtual Router Redundancy Protocol packets with the destination IPv6 address FF02::12.

To regulate any other traffic destined for the CPU, every CoPP policy has a class named `default` that can also be configured to regulate other traffic to the CPU or prevent other traffic from being delivered.




---

All IPsec traffic received by the CPU will be regulated by the `ipsec` class regardless of the encapsulated protocol.

---

## apply copp-policy

```
apply copp-policy { <NAME> | default }
no apply copp-policy <NAME>
```

### Description

Applies a CoPP policy to the switch, replacing the policy that is in effect. There may be a brief interruption in traffic flow to the management processor while the switch implements the change.

Enter the **no apply copp-policy <NAME>** command with the name of a CoPP policy to unapply a CoPP policy and apply the default CoPP policy. This will only take effect if the specified policy is actively applied. Since there must always be a CoPP policy applied, this command effectively attempts to replace the applied CoPP policy with the default CoPP policy. The default CoPP policy cannot be unapplied using this command.

| Parameter                 | Description                                                            |
|---------------------------|------------------------------------------------------------------------|
| <code>&lt;NAME&gt;</code> | Specifies the name of the policy to apply. Length: 1 to 64 characters. |
| <code>default</code>      | Applies the default policy.                                            |

### Usage

If the new policy cannot be applied (for example, due to a lack of hardware resources), the previous policy remains in effect. Use the [show copp-policy](#) command to determine which policy is in effect.

### Examples

Applying a policy named `My_CoppPolicy`:

```
switch(config)# apply copp-policy My_CoppPolicy
```

Applying the default policy:



```
switch(config)# apply copp-policy default
```

Unapplying a policy named My\_CoppPolicy:

```
switch(config)# no apply copp-policy My_CoppPolicy
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## class

```
class <CLASS> {drop | priority <PRIORITY> rate <RATE> [burst <BURST>]}
no class <CLASS> {drop | priority <PRIORITY> rate <RATE> [burst <BURST>]}
```

## Description

Adds a class to a CoPP policy. If the class exists, the existing class is modified. Changes made to an active (applied) policy take effect immediately.

When adding or modifying a class in an active policy, CoPP immediately activates the change on the switch. In cases where insufficient hardware resources exist to support a class or its action, CoPP fails to activate the changed class on the switch. When this failure occurs, the active configuration on the switch will be out of sync with its definition. To diagnose and remedy this situation:

- Use the [show copp-policy](#) command to determine which classes are out of sync between the active policy and its definition.
- Use the [reset copp-policy](#) command to synchronize the active policy with its definition. This synchronization changes the classes in the definition to match the classes in the active policy.

The **no** form of this command removes a class from a CoPP policy. Traffic for the removed class that is destined for the processor will be included in the default class. To stop a class of traffic from reaching the processor, set the class action to drop.

| Parameter | Description                         |
|-----------|-------------------------------------|
| <CLASS>   | Specifies the class to add or edit. |

| Parameter           | Description                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------|
| drop                | Drop packets matching the selected class.                                                                            |
| priority <PRIORITY> | Specifies the priority for packets matching the selected class. Range: 0 to 7.                                       |
| rate <RATE>         | Specifies the maximum rate, in packets per second (pps), for packets matching the selected class. Range: 1 to 99999. |
| burst <BURST>       | Specifies the maximum burst size, in packets, for packets matching the selected class. Range: 1 to 9999.             |

## Examples

Adding a class to handle LACP traffic with priority of 2 and rate of 2000:

```
switch(config-copp)# class lacp priority 2 rate 2000
```

Modifying the class to drop LLDP packets:

```
switch(config-copp)# class lldp drop
```

Removing the class that handles LLDP packets. LLDP traffic destined to the processor will be included in the default class.

```
switch(config-copp)# no class lldp
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-copp     | Administrators or local user group members with execution rights for this command. |

## clear copp-policy statistics

```
clear copp-policy statistics
```

### Description

Resets statistics for all CoPP classes to zero.

## Examples

Displaying and then resetting statistics for all classes in the active policy:

```
switch# show copp-policy statistics
Statistics for CoPP policy 'default':
Totals:
 bytes passed : 64000
 packets passed : 1000
 avg_packet_size_passed: 64
 bytes dropped : 96000
 packets dropped : 1500
 avg_packet_size_dropped: 64
Class: default
 bytes passed : 25600
 packets passed : 400
 avg_packet_size_passed: 64
 bytes dropped : 38400
 packets dropped : 600
 avg_packet_size_dropped: 64
Class: acl-logging
 bytes passed : 6400
 packets passed : 100
 avg_packet_size_passed: 64
 bytes dropped : 6400
 packets dropped : 100
 avg_packet_size_dropped: 64
Class: arp-broadcast
 bytes passed : 32000
 packets passed : 500
 avg_packet_size_passed: 64
 bytes dropped : 51200
 packets dropped : 800
 avg_packet_size_dropped: 64
<--OUTPUT OMITTED FOR BREVITY-->
switch# clear copp-policy statistics
switch# show copp-policy statistics
Statistics for CoPP policy 'default':
Totals:
 bytes passed : 0
 packets passed : 0
 avg_packet_size_passed: 0
 bytes dropped : 0
 packets dropped : 0
 avg_packet_size_dropped: 0
Class: default
 bytes passed : 0
 packets passed : 0
 avg_packet_size_passed: 0
 bytes dropped : 0
 packets dropped : 0
 avg_packet_size_dropped: 0
Class: acl-logging
 bytes passed : 0
 packets passed : 0
 avg_packet_size_passed: 0
 bytes dropped : 0
 packets dropped : 0
 avg_packet_size_dropped: 0
Class: arp-broadcast
 bytes passed : 0
 packets passed : 0
 avg_packet_size_passed: 0
 bytes dropped : 0
 packets dropped : 0
 avg_packet_size_dropped: 0
<--OUTPUT OMITTED FOR BREVITY-->
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# copp-policy

```
copp-policy {<NAME> | default [revert]]}
no copp-policy <NAME>
```

## Description

Creates a CoPP policy and switches to the **config-copp** context for the policy. Or, if the specified policy exists, switches to the **config-copp** context for the policy. A predefined policy, named **default**, contains factory default classes and is applied to the switch at first startup. This policy cannot be deleted, but its configuration can be changed.

The **no** form of this command removes a CoPP policy. If a policy is active (applied), it cannot be removed. It must be replaced with another policy before it can be removed.

| Parameter | Description                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NAME>    | Specifies the name of the policy to add or edit. Length: 1 to 64 characters. The name must not be a substring of any of the following reserved words: default, factory-default, commands, configuration, or statistics. |
| default   | Specifies the default CoPP policy. Use this default policy to configure the default policy.                                                                                                                             |
| revert    | Sets the default CoPP policy to its factory settings.                                                                                                                                                                   |

## Examples

Creating a policy named My\_CoppPolicy:

```
switch(config)# copp-policy My_CoppPolicy
switch(config-copp)#
```

Removing a policy named My\_CoppPolicy:

```
switch(config)# no copp-policy My_CoppPolicy
```

Setting the default policy to its factory settings:

```
switch(config)# copp-policy default revert
```

Unapplying the policy named My\_CoppPolicy:

```
switch(config)# no apply copp-policy My_CoppPolicy
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## default-class

default-class priority <PRIORITY> rate <RATE> [burst <BURST>]

### Description

Configures the default class that is automatically defined for all CoPP policies. The default class cannot be removed, but its configuration can be changed. The default class is applied to traffic that does not match any other class defined for a policy.

| Parameter           | Description                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------|
| priority <PRIORITY> | Specifies the priority for packets matching the selected class. Range: 0 to 7.                                       |
| rate <RATE>         | Specifies the maximum rate, in packets per second (pps), for packets matching the selected class. Range: 1 to 99999. |
| burst <BURST>       | Specifies the maximum burst size, in packets, for packets matching the selected class. Range: 1 to 9999.             |

### Example

Setting the default class to a priority of **2** and rate of **2000**:

```
switch(config-copp)# default-class priority 2 rate 2000
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-copp     | Administrators or local user group members with execution rights for this command. |

# reset copp-policy

```
reset copp-policy { <NAME> | default }
```

## Description

Resets an active CoPP policy to match the settings that are currently in effect for the active policy on the switch. Changes made to the active policy that could not be activated are removed from the active policy. When the switch fails to add or modify a class in an active CoPP policy, it is possible the active policy settings on the switch may be out of sync with those defined in the policy.

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| <NAME>    | Specifies the name of the policy to reset. Length: 1 to 64 characters. |
| default   | Resets the default policy to match its active settings.                |

## Examples

Resetting a policy named My\_CoppPolicy:

```
switch# show copp-policy My_CoppPolicy
class drop priority rate pps burst pkts hardware rate pps

igmp 6 5000 60 5000
lacp 2 2000 1000 2000
default 1 6000 70 6000
switch# config terminal
switch(config)# copp-policy My_CoppPolicy
switch(config-copp)# class stp priority 4 rate 4000 burst 60
switch(config-copp)# do show copp-policy My_CoppPolicy
class drop priority rate pps burst pkts hardware rate pps

igmp 6 5000 60 5000
lacp 2 2000 1000 2000
default 1 6000 70 6000
% Warning: user-specified classes in CoPP policy My_CoppPolicy do not match
active configuration.
switch(config-copp)# do show copp-policy My_CoppPolicy configuration
class drop priority rate pps burst pkts applied

igmp 6 5000 60 yes
lacp 2 2000 1000 yes
stp 4 4000 60 no
default 1 6000 70 yes
% Warning: user-specified classes in CoPP policy My_CoppPolicy do not match
active configuration.
switch(config-copp)# exit
switch(config)# reset copp-policy My_CoppPolicy
switch(config)# do show copp-policy My_CoppPolicy
class drop priority rate pps burst pkts hardware rate pps

igmp 6 5000 60 5000
lacp 2 2000 1000 2000
default 1 6000 70 6000
```

Resetting the default policy:

```
switch(config)# reset copp-policy default
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show copp-policy

```
show copp-policy [<NAME> | default] [commands] [configuration] [vsx-peer]
```

### Description

Shows CoPP policy settings for a specific CoPP policy. When entered without specifying either a name or the `default` parameter, shows all the CoPP policy settings that are active on the switch and have successfully been programmed into the hardware.

A warning is displayed if:

- The active and user-specified applications of a policy do not match.
- The active and user-specified configurations of a policy do not match.

| Parameter     | Description                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <NAME>        | Specifies the name of the policy for which to display settings. Length: 1 to 64 characters.                                                                                                                                      |
| default       | Displays CoPP settings for the default policy.                                                                                                                                                                                   |
| commands      | Displays output as CLI commands.                                                                                                                                                                                                 |
| configuration | Displays user-specified CoPP settings and <b>not</b> the active settings.                                                                                                                                                        |
| vsx-peer      | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

Displaying the CoPP policies defined in the configuration and the active application:

```

switch#
show copp-policy
applied copp_policy_name

My_CoppPolicy
applied default
switch#

```

Displaying the active configuration of all CoPP policies as CLI commands:

```

switch# show copp-policy commands
copp-policy My_CoppPolicy
 class igmp priority 6 rate 5000 burst 60
 class lacp priority 2 rate 2000 burst 1000
 default-class priority 1 rate 6000 burst 70
copp-policy default
 class acl-logging priority 0 rate 50 burst 50
 class arp-broadcast priority 3 rate 7000 burst 7000
 class arp-unicast priority 4 rate 2500 burst 2500
 class bfd priority 7 rate 1000 burst 1000
 <--OUTPUT OMITTED FOR BREVITY-->
 default-class priority 1 rate 1000 burst 500
apply copp-policy default
switch#

```

Displaying the default policy:

```

switch# show copp-policy default
class drop priority rate pps burst pkts hardware rate pps

acl-logging 0 50 50 50
arp-broadcast 3 7000 7000 7000
arp-unicast 4 2500 2500 2500
bfd 7 1000 1000 1000
 <--OUTPUT OMITTED FOR BREVITY-->
default 1 1000 500 1000

```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |



# show copp-policy factory-default

show copp-policy factory-default [commands] [vsx-peer]

## Description

Display the configuration for the factory-default CoPP policy.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| commands  | Displays output as CLI commands.                                                                                                                                                                                                 |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

Displaying the factory-default policy:

```
switch# show copp-policy factory-default
class drop priority rate pps burst pkts

acl-logging 0 50 50
arp-broadcast 3 7000 7000
arp-unicast 4 2500 2500
bfd 7 1000 1000
 <--OUTPUT OMITTED FOR BREVITY-->
default 1 1000 500
```

Displaying the active configuration of **My\_CoppPolicy** (**My\_CoppPolicy** is applied):

```
switch# config terminal
switch(config)# apply copp-policy My_CoppPolicy
switch(config)# do show copp-policy My_CoppPolicy
class drop priority rate pps burst pkts hardware rate pps

igmp 6 5000 60 5000
lacp 2 2000 1000 2000
default 1 6000 70 6000
```

Displaying the active configuration of **My\_CoppPolicy** as CLI commands:

```
switch# show copp-policy My_CoppPolicy commands
copp-policy My_CoppPolicy
 class igmp priority 6 rate 5000 burst 60
 class lacp priority 2 rate 2000 burst 1000
 default-class priority 1 rate 6000 burst 70
apply copp-policy My_CoppPolicy
```

Displaying the user-specified configuration of **My\_CoppPolicy**:

```
switch# show copp-policy My_CoppPolicy configuration
class drop priority rate pps burst pkts applied
```

```

igmp 6 5000 60 yes
lacp 2 2000 1000 yes
default 1 6000 70 yes

```

Displaying the user-specified configuration of **My\_CoppPolicy** as CLI commands:

```

switch# show copp-policy My_CoppPolicy commands configuration
copp-policy My_CoppPolicy
 class igmp priority 6 rate 5000 burst 60
 class lacp priority 2 rate 2000 burst 1000
 default-class priority 1 rate 6000 burst 70
apply copp-policy My_CoppPolicy

```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show copp-policy statistics

`show copp-policy statistics [class <CLASS> | default-class | non-zero] [vsx-peer]`

### Description

Displays statistics for all classes, a single class, or all classes with non-zero statistics in the active CoPP policy.

| Parameter     | Description                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <CLASS>       | Specifies the <a href="#">class</a> for which to display statistics.                                                                                                                                                             |
| default-class | Displays statistics for the default class.                                                                                                                                                                                       |
| non-zero      | Displays statistics for all classes with non-zero statistics.                                                                                                                                                                    |
| vsx-peer      | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Usage

If a single class is specified, the priority, rate, and burst size that has been programmed in hardware for that class will be shown. This command will fail with an alert if the user specifies a class that is not configured for the actively applied CoPP policy.

## Examples

Applying the **default** CoPP policy and displaying statistics for all classes in the actively applied policy:



---

The rate displayed is the actual rate in hardware.

---

```
switch# config terminal
switch(config)# apply copp-policy default
switch(config)# exit
switch# show copp-policy statistics
Statistics for CoPP policy 'default':
Totals:
 bytes passed : 64000 bytes dropped : 96000
 packets passed : 1000 packets dropped : 1500
 avg_packet_size_passed: 64 avg_packet_size_dropped: 64
Class: default
 bytes passed : 25600 bytes dropped : 38400
 packets passed : 400 packets dropped : 600
 avg_packet_size_passed: 64 avg_packet_size_dropped: 64
Class: acl-logging
 bytes passed : 6400 bytes dropped : 6400
 packets passed : 100 packets dropped : 100
 avg_packet_size_passed: 64 avg_packet_size_dropped: 64
Class: arp-broadcast
 bytes passed : 32000 bytes dropped : 51200
 packets passed : 500 packets dropped : 800
 avg_packet_size_passed: 64 avg_packet_size_dropped: 64
 <--OUTPUT OMITTED FOR BREVITY-->
```

Displaying statistics for the default class in the active policy:

```
switch(config)# show copp-policy statistics default-class
Statistics for CoPP policy 'default':
Class: default
Description: Default
 priority : 1
 rate (pps) : 1000
 burst size (pkts) : 500

 bytes passed : 25600 bytes dropped : 38400
 packets passed : 400 packets dropped : 600
 avg_packet_size_passed: 64 avg_packet_size_dropped: 64
```

Displaying statistics for the class **arp-broadcast** in the actively applied policy:

```
switch# show copp-policy statistics class arp-broadcast
Statistics for CoPP policy 'default':
Class: arp-broadcast
Description: Address Resolution Protocol broadcast
 priority : 3
```

```
rate (pps) : 7000
burst size (pkts) : 7000

bytes passed : 32000 bytes dropped : 51200
packets passed : 500 packets dropped : 800
avg_packet_size_passed : 64 avg_packet_size_dropped: 64
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show tech copp

show tech copp

### Description

Displays the output of all show commands supported by CoPP.

### Examples

Capturing the command output into a local file:

```
switch# show tech copp local-file
Show Tech output stored in local-file. Please use 'copy show-tech local-file' to
copy-out this file.

switch# copy show-tech local-file ?
 REMOTE_URL URL of syntax
 {tftp://|sftp://USER@}{IP|HOST}[:PORT][;blocksize=VAL]/FILE
 STORAGE_URL URL of syntax usb:/file
switch# copy show-tech local-file
```



For more information on features that use this command, refer to the CoPP Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

clear debug buffer

clear debug buffer

Description

Clears all debug logs. Using the **show debug buffer** command will only display the logs generated after the **clear debug buffer** command.

Examples

Clearing all generated debug logs:

```
switch# show debug buffer

show debug buffer

2018-10-14:09:10:58.558710|lldpd|LOG_DEBUG|MSTR||LLDP|LLDP_CONFIG|No Port cfg
changes
2018-10-14:09:10:58.558737|lldpd|LOG_DEBUG|MSTR||LLDP|LLDP_EVENT|lldpd_stats_run
entered at time 8257199
2018-10-14:09:10:58.569317|lldpd|LOG_DEBUG|MSTR||LLDP|LLDP_CONFIG|No Port cfg
changes
2018-10-14:09:11:21.881907|hpe-sysmond|LOG_INFO|MSTR||SYSMON|SYSMON_CONFIG|Sysmon
poll interval changed to 32

switch# clear debug buffer
switch# show debug buffer

show debug buffer

2018-10-14:09:13:24.481407|hpe-sysmond|LOG_INFO|MSTR||SYSMON|SYSMON_CONFIG|Sysmon
poll interval changed to 51
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### debug {all | <MODULE-NAME>}

```
debug {all | <MODULE-NAME>} [<SUBMODULE-NAME>] [severity
 (emer|crit|alert|err|notice|warning|info|debug)] {port <PORT-NAME> |
 vlan <VLAN-ID> | ip <IP-ADDRESS> | mac <MAC-ADDRESS> |
 vrf <VRF-NAME> | instance <INSTANCE-ID>}
no debug {all | <MODULE-NAME>} [<SUBMODULE-NAME>] {port | vlan | ip | mac |
 vrf | instance}
```

### Description

Enables debug logging for modules or submodules by name, with optional filtering by specific criteria. The **no** form of this command disables debug logging.

| Parameter                                                | Description                                                                                                                                                                         |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all                                                      | Enables debug logging for all modules.                                                                                                                                              |
| <MODULE-NAME>                                            | Enables debug logging for a specific module. For a list of supported modules, enter the <b>debug</b> command followed by a space and a question mark (?).                           |
| <SUBMODULE-NAME>                                         | Enables debug logging for a specific submodule. For a list of supported submodules, enter the <b>debug &lt;MODULE-NAME&gt;</b> command followed by a space and a question mark (?). |
| severity (emer crit alert err notice warning info debug) | Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is <b>debug</b> . Optional.                                        |
| emer                                                     | Specifies storage of debug logs with a severity level of <b>emergency</b> only.                                                                                                     |
| crit                                                     | Specifies storage of debug logs with severity level of <b>critical</b> and above.                                                                                                   |
| alert                                                    | Specifies storage of debug logs with severity level of <b>alert</b> and above.                                                                                                      |
| err                                                      | Specifies storage of debug logs with severity level of <b>error</b> and above.                                                                                                      |
| notice                                                   | Specifies storage of debug logs with severity level of <b>notice</b> and above.                                                                                                     |
| warning                                                  | Specifies storage of debug logs with severity level of <b>warning</b> and above.                                                                                                    |
| info                                                     | Specifies storage of debug logs with severity level of <b>info</b> and above.                                                                                                       |

| Parameter              | Description                                                                           |
|------------------------|---------------------------------------------------------------------------------------|
| debug                  | Specifies storage of debug logs with severity level of <b>debug</b> (default).        |
| port                   | Displays debug logs for the specified port, for example <b>1/1/1</b> .                |
| vlan <VLAN-ID>         | Displays debug logs for the specified VLAN. Provide a VLAN from 1 to 4094.            |
| ip <IP-ADDRESS>        | Displays debug logs for the specified IP Address.                                     |
| mac <MAC-ADDRESS>      | Displays debug logs for the specified MAC Address, for example <b>A:B:C:D:E:F</b> .   |
| vrf <VRF-NAME>         | Displays debug logs for the specified VRF.                                            |
| instance <INSTANCE-ID> | Displays debug logs for the specified instance. Provide an instance ID from 1 to 255. |

## Examples

```
switch# debug all
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## debug db

```
debug db {all | sub-module} [level <MINIMUM-SEVERITY>] [filter]
```

```
no debug db {all | sub-module} [level <MINIMUM-SEVERITY>] [filter]
```

## Description

Enables or disables debug logging for a db module or submodules, with an option to filter by specific criteria.

The **no** form of this command disables debug logging for the db module or submodule.



| Parameter                                                             | Description                                                                                                                                  |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <code>all</code>                                                      | Enables all submodules for the db log.                                                                                                       |
| <code>sub-module</code>                                               | Enables debug logging for supported submodules. Specify <b>rx</b> or <b>tx</b> debug logs.                                                   |
| <code>filter</code>                                                   | Specifies supported filters for the db log. Specify <b>table</b> , <b>column</b> , or <b>client</b> . Optional                               |
| <code>severity (emer crit alert err notice warning info debug)</code> | Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is <b>debug</b> . Optional. |
| <code>emer</code>                                                     | Specifies storage of debug logs with a severity level of <b>emergency</b> only.                                                              |
| <code>crit</code>                                                     | Specifies storage of debug logs with severity level of <b>critical</b> and above.                                                            |
| <code>alert</code>                                                    | Specifies storage of debug logs with severity level of <b>alert</b> and above.                                                               |
| <code>err</code>                                                      | Specifies storage of debug logs with severity level of <b>error</b> and above.                                                               |
| <code>notice</code>                                                   | Specifies storage of debug logs with severity level of <b>notice</b> and above.                                                              |
| <code>warning</code>                                                  | Specifies storage of debug logs with severity level of <b>warning</b> and above.                                                             |
| <code>info</code>                                                     | Specifies storage of debug logs with severity level of <b>info</b> and above.                                                                |
| <code>debug</code>                                                    | Specifies storage of debug logs with severity level of <b>debug</b> (default).                                                               |

## Usage

DBlog is a high performance, configuration, and state database server logging infrastructure where a user can log the transactions which are sent or received by clients to the configuration and state database server. It can be enabled through the CLI and REST, and also supports filters where a user can filter out logs on the basis of table, column, or client. It is helpful for debugging when the user wants to debug an issue with a particular client, table, or column combination. It is not enabled by default. A combination of filters can also be applied to filter out messages based on table, column, and client.

There are three submodules for the "db" module:

1. **all**: When All is enabled, no filters are applied to any of the debug logs, even if other submodules are configured with filters.
2. **tx**: If enabled, only the replies and notifications sent out for the initial and incremental updates are logged.
3. **rx**: If enabled, only the transactions sent to the configuration and state database server are logged.

The keyword **all** may be used to enable or disable debug logging for all sub-modules. Also a combination of filters can be used to filter the message types.

If the table or client filter is applied, then the messages belonging to this specific table or client will be logged. The column filter can also be applied to further filter messages on a table, providing a mechanism to filter messages on a column. The table and client filter can be used in combination or separately, but column can only be used in conjunction with table.

## Examples

Configuring all submodules with severity **debug**:

```
switch# debug db all severity debug
```

Configuring the **tx** submodule with **table Interface** filter and severity **debug**:

```
switch# debug db tx table Interface severity debug
```

Configuring the **rx** submodule with **table Interface column statistics** filter and severity **debug**:

```
switch# debug db rx table Interface column statistics severity debug
```

Disabling the **rx** submodule:

```
switch# no debug db rx
```

Disabling the **tx** submodule **table Interface**:

```
switch# no debug db tx table Interface
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## debug destination

```
debug destination {syslog | file | console | buffer} [severity
(emer|crit|alert|err|notice|warning|info|debug)]
no debug destination {syslog | file | console}
```

## Description

Sets the destination for debug logs and the minimum severity level for each destination

The **no** form of this command unsets the destination for debug logs.

| Parameter                                                | Description                                                                                                                                  |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| {syslog   file   console   buffer}                       | Selects the destination to store debug logs. Required.                                                                                       |
| syslog                                                   | Specifies that the debug logs are stored in the <b>syslog</b> .                                                                              |
| file                                                     | Specifies that debug logs are stored in <b>file</b> .                                                                                        |
| console                                                  | Specifies that debug logs are stored in <b>console</b> .                                                                                     |
| buffer                                                   | Specifies that debug logs are stored in <b>buffer</b> (default).                                                                             |
| severity {emer crit alert err notice warning info debug} | Selects the minimum severity log level for the destination. If a severity is not provided, the default log level is <b>debug</b> . Optional. |
| emer                                                     | Specifies storage of debug logs with a severity level of <b>emergency</b> only.                                                              |
| crit                                                     | Specifies storage of debug logs with severity level of <b>critical</b> and above.                                                            |
| alert                                                    | Specifies storage of debug logs with severity level of <b>alert</b> and above.                                                               |
| err                                                      | Specifies storage of debug logs with severity level of <b>error</b> and above.                                                               |
| notice                                                   | Specifies storage of debug logs with severity level of <b>notice</b> and above.                                                              |
| warning                                                  | Specifies storage of debug logs with severity level of <b>warning</b> and above.                                                             |
| info                                                     | Specifies storage of debug logs with severity level of <b>info</b> and above.                                                                |
| debug                                                    | Specifies storage of debug logs with severity level of <b>debug</b> (default).                                                               |

## Usage

Events that have a severity equal to or higher than the configured severity level are stored in the designated destination. The product defaults to **buffer** for destination and **debug** as a severity level.

## Examples

```
switch# debug destination syslog severity alert
switch# debug destination console severity info
switch# debug destination file severity warning
```

```
switch# debug destination buffer severity err
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# diag event-trap-disable

```
diag event-trap-disable <EVENT-IDS>
```

```
no diag event-trap-disable <EVENT-IDS>
```

## Description

Prevents the specific event notifications from being sent as traps to the SNMP management stations. The **no** form of this command disables this feature and reenables the notification of events to be sent as traps.

| Parameter   | Description                                  |
|-------------|----------------------------------------------|
| <EVENT-IDS> | Specify up to five comma separated Event IDs |

## Usage

To modify the traps to be disabled, such as changing the existing list of event IDs or removing an event ID from the blocked trap list, first completely remove previously configured disabled traps using the CLI command **no diag event-trap-disable <EVENT-ID>**. After that, reconfigure the new event IDs or set of event IDs for the changes to take effect.

The command to disable traps cannot be issued via network management systems such as SNMP, the REST API, HPE Aruba Networking Fabric Composer or HPE Aruba Networking Central. The configuration to disable event-traps is not persistent across reboots, and traps will be enabled again after the switch reboots.



Do not disable default event trap IDs, as this can cause conflicts with a switch configuration with default traps enabled.

## Examples

Disable and then reenable event traps 1223 and 1224.

```
switch# diagnostics
switch# diag event-trap-disable 1223,1224
switch# no diag event-trap-disable 1223,1224
```

Change the list of disabled event traps.

```
switch# diagnostics
switch# diag event-trap-disable 1223,1224
switch# no diag event-trap-disable 1223,1224
switch# diag event-trap-disable 1225,1226
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release    | Modification |
|------------|--------------|
| 10.15.1010 | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show debug

show debug [vsx-peer]

### Description

Displays the enabled debug types.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

```
switch# show debug
```

-----

-

```

module sub_module severity vlan port ip mac instance vrf

-
all all err 1 1/1/1 10.0.0.1 1a:2b:3c:4d:5e:6f 2
abcd

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show debug buffer

```

show debug buffer [module <MODULE-NAME> | severity
(emer|crit|alert|err|notice|warning|info|debug)]

```

## Description

Displays debug logs stored in the specified debug buffer with optional filtering by module or severity.

| Parameter                                                | Description                                                                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <MODULE-NAME>                                            | Filters debug logs displayed by the specified module name.                                |
| severity (emer crit alert err notice warning info debug) | Displays debug logs with a specified severity level. Defaults to <b>debug</b> . Optional. |
| emer                                                     | Displays debug logs with a severity level of <b>emergency</b> only.                       |
| crit                                                     | Displays debug logs with a severity level of <b>critical</b> and above.                   |
| alert                                                    | Displays debug logs with a severity level of <b>alert</b> and above.                      |
| err                                                      | Specifies storage of debug logs with severity level of <b>error</b> and above.            |
| notice                                                   | Specifies storage of debug logs with severity level of <b>notice</b> and above.           |
| warning                                                  | Displays debug logs with a severity level of <b>warning</b> and above.                    |

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| info      | Displays debug logs with a severity level of <b>info</b> and above.  |
| debug     | Displays debug logs with a severity level of <b>debug</b> (default). |

## Examples

```
switch# show debug buffer

show debug buffer

2017-03-06:06:51:15.089967|hpe-sysmond|SYSMON|SYSMON_CONFIG|LOG_INFO|Sysmon poll
interval changed to 20
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show debug destination

show debug destination [vsx-peer]

## Description

Displays the configured debug destination and severity.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

```
switch# show debug destination
```

```

show debug destination

```

```
CONSOLE:info
FILE:warning
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |



## ip dhcp

ip dhcp  
no ip dhcp

### Description

Enables the DHCP client on the management interface or any interface VLAN to automatically obtain an IP address from a DHCP server on the network. By default, the DHCP client is enabled on the management interface and VLAN 1.

The **no** form of the command disables DHCP mode and is supported only on interface VLANs; it is not supported on the management interface.

### Examples

Enabling the DHCP client on the management interface:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip dhcp
switch(config-if-mgmt)# no shutdown
```

Enabling the DHCP client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp
switch(config-if-vlan)# no shutdown
```

Disabling the DHCP client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip dhcp
```

Enabling the DHCP client on the interface vlan 4 under non-default VRF:

```
switch(config)# interface vlan 4
switch(config-if-vlan)# vrf attach red
switch(config-if-vlan)# ip dhcp
```

If the interface is not enabled, you can enable it by entering the `no shutdown` command.



---

DHCP client can be enabled on one or more user VLANs.

---



---

For more information on features that use this command, refer to the IP Services Guide for your switch model.

---

## General Limitations

1. ZTP (Zero Touch Provisioning) options from a DHCP server are only supported on VLAN 1. These options will be ignored if received on any other VLAN.
2. CoP and HTTPS-proxy DHCP options should be received on only one DHCP client-enabled VLAN. If multiple VLANs receive the same option, the selection of the VLAN from which the options are applied is non-deterministic. Therefore, configuring multiple VLANs to receive these options is not recommended.
3. It is recommended to limit the number of DHCP client VLANs in a system to 32. This total includes both DHCPv4 and DHCPv6 client instances.
4. The `ip dhcp option broadcast-flag` configuration must be enabled to successfully obtain DHCP IP addresses across multiple VLANs when the default gateway route is present.

## Command History

| Release          | Modification                                                                        |
|------------------|-------------------------------------------------------------------------------------|
| 10.17            | Support enabled on one or more user VLANs.                                          |
| 10.16.1000       | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.07 or earlier | --                                                                                  |

## Command Information

| Platforms     | Command context                                            | Authority                                                                          |
|---------------|------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config-if-mgmt</code><br><code>config-if-vlan</code> | Administrators or local user group members with execution rights for this command. |

## ipv6 dhcp

`ipv6 dhcp`  
`no ipv6 dhcp`

### Description

Configure to enable DHCPv6 mode on a VLAN. In DHCPv6 Mode, the VLAN will get a DHCP-Server allocated IPv6 address along with DNS and NTP attributes.

The **no** form of the command disables DHCP mode and is supported only on interface VLANs; it is not supported on the management interface.



ZTPv6 attributes are included in the request packet, but they are not utilized by ZTP on the data port. Currently, ZTPv6 attributes are only supported on the management port. Also, IPv6 addresses assigned through DHCPv6 only support a /64 prefix.

### Examples

Enabling the DHCPv6 client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 dhcp
```

Enabling the DHCPv6 on two VLANs:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 dhcp

switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 dhcp
```

Enabling the DHCPv6 client on the interface vlan 4 under non-default VRF:

```
switch(config)# interface vlan 4
switch(config-if-vlan)# vrf attach red
switch(config-if-vlan)# ipv6 dhcp
```

Disabling the DHCPv6 client on the interface vlan 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 dhcp
```

If the interface is not enabled, you can enable it by entering the `no shutdown` command.



---

For more information on features that use this command, refer to the IP Services Guide for your switch model.

---

## General Limitations

1. ZTP (Zero Touch Provisioning) options from a DHCP server are only supported on VLAN 1. These options will be ignored if received on any other VLAN.
2. CoP and HTTPS-proxy DHCP options should be received on only one DHCP client-enabled VLAN. If multiple VLANs receive the same option, the selection of the VLAN from which the options are applied is non-deterministic. Therefore, configuring multiple VLANs to receive these options is not recommended.
3. It is recommended to limit the number of DHCP client VLANs in a system to 32. This total includes both DHCPv4 and DHCPv6 client instances.
4. The `ip dhcp option broadcast-flag` configuration must be enabled to successfully obtain DHCP IP addresses across multiple VLANs when the default gateway route is present.

## Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 10.17      | Support added for DHCPv6 on multiple VLANs.                                         |
| 10.16.1000 | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.15      | Command was introduced.                                                             |

## Command Information

| Platforms     | Command context                  | Authority                                                                          |
|---------------|----------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if-mgmt<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## ip dhcp option

```
ip dhcp option [host-name | broadcast-flag]
no ip dhcp option [host-name | broadcast-flag]
```

### Description

This command enables the DHCP client host name and broadcast flag globally.

If the **ip dhcp option broadcast-flag** command is enabled, then the DHCP offer and ack packets in the DHCP requests will be treated as broadcast packets. These packets will not be forwarded due to the presence of a default static route.

The **no** form of this command globally disables the host name and DHCP client broadcast flag options.



The **ip dhcp option broadcast-flag** command should be configured before configuring the **ip dhcp** command.

### Example

Enabling the DHCP client broadcast flag globally:

```
switch(config)# ip dhcp option
broadcast-flag DHCP Client broadcast-flag option (Default:disabled)
host-name DHCP Client hostname option
switch(config)# ip dhcp option
% Command incomplete.
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp
switch(config-if-vlan)# ip dhcp op
% There is no matched command.
switch(config-if-vlan)# ip dhcp op
Invalid input: ip
switch(config-if-vlan)#
```

Enabling the DHCP client host name globally:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp option host-name
```

Disabling the DHCP client broadcast flag globally:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip dhcp option broadcast-flag
```

Disabling the DHCP client host name globally:

```
switch(config)# ip dhcp option
broadcast-flag DHCP Client broadcast-flag option (Default:disabled)
```

```

host-name DHCP Client hostname option
switch(config)# ip dhcp option
% Command incomplete.
switch(config)# interface vlan 1
switch(config-if-vlan)# ip dhcp
switch(config-if-vlan)# no ip dhcp option host-name
% There is no matched command.
switch(config-if-vlan)# ip dhcp op
Invalid input: ip
switch(config-if-vlan)#

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 10.16.1000 | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.13.1000 | Command Introduced                                                                  |

## Command Information

| Platforms     | Command context                  | Authority                                                                          |
|---------------|----------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if-mgmt<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## ip dhcp preferred-vlan

```

ip dhcp preferred-vlan <VLAN-ID> [vrf <VRF-NAME>]
no ip dhcp preferred-vlan vlan <VLAN-ID> [vrf <VRF-NAME>]

```

### Description

Specifies the preferred VLAN for DHCP client options, including DNS, NTP, and Default Gateway. The preferred VLAN is the VLAN used to select DHCP client options within a specified VRF when multiple VLANs have DHCP client enabled in the same VRF. If no VRF is specified, the configuration applies to the default VRF. In cases where the preferred VLAN is not explicitly configured, the lowest VLAN with DHCP client enabled will be automatically selected.

The **no** form of the command removes the preferred VLAN configuration and restores the default behavior.

| Parameter  | Description                                                         |
|------------|---------------------------------------------------------------------|
| <VLAN-ID>  | VLAN ID to set as preferred VLAN. VLAN identifier range: 1 to 4094. |
| <VRF-NAME> | Specifies the VRF in which the preferred VLAN should be configured. |

## General Considerations

If the preferred VLAN configuration status is not *success*, the DHCP client-enabled VLAN with the lowest VLAN ID will be used for DHCP attribute selection.

Use the command `show ip dhcp preferred-vlan` to check the configuration status.

The preferred or lowest VLAN will be inactive in the following scenarios:

- a. When the DHCP interface is in a shutdown state and corresponds to the preferred or lowest VLAN ID.
- b. When a static IP is configured on an interface that also has DHCP enabled — the static IP takes precedence over DHCP.
- c. When DHCP attributes are not received from the server on the preferred or lowest VLAN.

## Examples

Selecting VLAN 1 as the preferred VLAN:

```
switch(config)# ip dhcp preferred-vlan 1
```

Selecting VLAN 10 as the preferred VLAN with VRF name:

```
switch(config)# ip dhcp preferred-vlan 10 vrf red
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## show ip dhcp

```
show ip dhcp
```

### Description

Displays DHCP IPv4 information on the ports.

### Examples

Displaying the DHCP IPv4 information on the ports:

```
switch# show ip dhcp
```

```
DHCP Options: Broadcast-flag, Hostname
```

| INTERFACE-NAME | ADDRESS          | DEFAULT_GATEWAY | DOMAIN_NAME | VRF     | DNS-SERVERS                     |
|----------------|------------------|-----------------|-------------|---------|---------------------------------|
| -----          |                  |                 |             |         |                                 |
| vlan1          | 10.254.239.10/27 |                 | domain.com  | default | 50.0.0.2,<br>50.0.0.3, 50.0.0.4 |



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification                                                                        |
|------------------|-------------------------------------------------------------------------------------|
| 10.16.1000       | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.13.1000       | The output parameters, <b>Broadcast-flag</b> and <b>Hostname</b> were introduced.   |
| 10.09 or earlier | Command introduced.                                                                 |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ipv6 dhcp

```
show ipv6 dhcp
```

### Description

This command displays DHCP IPv6 information on the ports.

### Examples

Displaying the DHCP IPv6 information on the ports:

```
6410(config)# show ipv6 dhcp

VRF default

Interface vlan1

IPv6 address : 3013::1050/64
Domain search : paramv6.org, test1.in, test2.in, test3.in, test4.in, test5.in
DNS servers : 3013::100, 3013::101, 3013::102
NTP servers : 3013::201, 3013::202
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release    | Modification                                                                        |
|------------|-------------------------------------------------------------------------------------|
| 10.16.1000 | Support added for the 8100, 832x, 8360, 8400, 9300, 9300S, and 10000 Switch Series. |
| 10.15      | Command was introduced.                                                             |

## Command Information

| Platforms     | Command context                  | Authority                                                                          |
|---------------|----------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if-mgmt<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

# show ip dhcp preferred-vlan

```
show ip dhcp preferred-vlan [{vrf <VRF-NAME> | all-vrfs}]
```

## Description

Displays the preferred DHCP client VLANs configured on the system.

| Parameter      | Description                           |
|----------------|---------------------------------------|
| vrf <VRF-NAME> | Show information for a specified VRF. |
| all-vrf        | Show information for all VRFs.        |

## Examples

Displaying the DHCP information for the preferred VLAN and VRF red:

```
switch# show ip dhcp preferred-vlan vrf red
VRF Preferred-VLAN Config-status

red 10 L3 interface not found
```

Displaying the DHCP information for the all VRFs:

```
switch# show ip dhcp preferred-vlan all-vrfs
VRF Preferred-VLAN Config-status

default 1 Success
red 9 VRF Mismatch
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.



## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## dhcp-relay

```
dhcp-relay
no dhcp-relay
```

### Description

Enables DHCP relay support. DHCP relay is enabled by default. DHCP relay is not supported on the management interface.

The **no** form of this command disables DHCP relay (and DHCP relay option 82) support.

### Examples

This example enables DHCP relay support.

```
switch(config)# dhcp-relay
```

This example removes DHCP relay support.

```
switch(config)# no dhcp-relay
```



---

For more information on features that use this command, refer to the IP Services Guide for your switch model.

---

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-relay hop-count-increment

```
dhcp-relay hop-count-increment
no dhcp-relay hop-count-increment
```

### Description

Enables the DHCP relay hop count increment feature, which causes the DHCP relay agent to increment the hop count in all relayed DHCP packets. Hop count is enabled by default.

The **no** form of this command disables the hop count increment feature.

## Examples

Enabling the hop count increment feature.

```
switch(config)# dhcp-relay hop-count-increment
```

Disabling the hop count increment feature.

```
switch(config)# no dhcp-relay hop-count-increment
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-relay l2vpn-clients

```
dhcp-relay l2vpn-clients
no dhcp-relay l2vpn-clients
```

### Description

Enables forwarding of packets from L2 VPN clients. Forwarding is enabled by default. Best practices is to disable this configuration on all the VXLAN tunnel endpoints (VTEPs), to avoid forwarding duplicate DHCP requests to the server.

The **no** form of this command disables forwarding of packets from L2 VPN clients.

### Usage

In Asymmetric/Symmetric Integrated Routing and Bridging (IRB) VXLAN deployments with a VLAN extension in subset of VTEPs, client DHCP broadcast requests are received by all the VTEPs where a client VLAN is configured. A DHCP-Relay agent on those VTEPs forward DHCP packets to configured DHCP server(s). As DHCP requests are forwarded by multiple DHCP relay agents, the DHCP server receives duplicate copies of the same packet.

When a VLAN is mapped to an L2VNI, any client requests that are received from that VLAN are considered as L2VPN clients.

When **dhcp-relay l2vpn-clients** is configured, MAC check validation is not performed on the VLAN. All requests are being sent to the DHCP server. This can increase the load on the DHCP Server

When **no dhcp-relay l2vpn-clients** is configured, MAC check validation is performed on the VLAN. When clients request an IP, a MAC check is performed and fails for the first packet as there is no MAC in DB by that time. The requests are dropped until the MAC Address is programmed learned . Once it is programmed learned, requests from the client are successful because the MAC entry is already present. It is recommended to enable **dhcp-relay l2vpn-clients** on a few switches in the network topology if there are client systems that is sensitive to DHCP packet loss.

## Example

Enabling forwarding of packets from L2 VPN clients.

```
switch(config)# dhcp-relay l2vpn-clients
switch(config)# no dhcp-relay l2vpn-clients
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-relay option 82

```
[no] dhcp-relay option 82
 replace {ip | mac | validate}
 drop {ip | mac | validate}
 keep {ip | mac}
 source-interface
 circuit-id port-id
 validate {drop {ip | mac}}
```

## Description

Configures the behavior of DHCP relay option 82. A DHCP relay agent can receive a message from another DHCP relay agent having option 82. The relay information from the previous relay agent is replaced by default.

The **no** form of this command disables the DHCP relay option 82 configurations. Option 82 is disabled when DHCP relay is disabled globally. When DHCP relay is re-enabled, option 82 also needs to be re-enabled using the **dhcp-relay option 82** command.



DHCP Relay is supported over VXLAN with both IPv4 and IPv6 underlay.

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>replace</code>            | Replace the existing option 82 field in an inbound client DHCP packet with the information from the switch. The remote ID and circuit ID information from the first relay agent is lost. Default.                                                                                                                                                                                                                                            |
| <code>drop</code>               | Drop any inbound client DHCP packet that contains option 82 information.                                                                                                                                                                                                                                                                                                                                                                     |
| <code>keep</code>               | Keep the existing option 82 field in an inbound client DHCP packet. The remote ID and circuit ID information from the first relay agent is preserved.                                                                                                                                                                                                                                                                                        |
| <code>source-interface</code>   | Configures the DHCP relay to use a configured source IP address for inter-VRF server reachability. Set the source IP address with the command <code>ip source-interface</code> .                                                                                                                                                                                                                                                             |
| <code>circuit-id port-id</code> | Configures the circuit ID and remote ID options.<br><br><b>NOTE:</b> When enabled, DHCP Relay, unlike DHCP Snooping, drops packets from single-homed clients connected to only one switch in the VSX pair if they arrive on the VSX Secondary, unless the <code>dhcp-relay vsx active-active</code> command is enabled. To avoid this, connect single-homed clients to the VSX Primary or enable <code>dhcp-relay vsx active-active</code> . |
| <code>validate</code>           | Validate option 82 information in DHCP server responses and drop invalid responses.                                                                                                                                                                                                                                                                                                                                                          |
| <code>ip</code>                 | Use the IP address of the interface on which the client DHCP packet entered the switch as the option 82 remote ID.                                                                                                                                                                                                                                                                                                                           |
| <code>mac</code>                | Use the MAC address of the switch as the option 82 remote ID. Default.                                                                                                                                                                                                                                                                                                                                                                       |

## Example

This example enables DHCP option 82 support and replaces all option 82 information with the values from the switch, with the switch MAC address as the remote ID.

```
switch(config)# dhcp-relay option 82 replace mac
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification                                            |
|------------------|---------------------------------------------------------|
| 10.17            | The <b>circuit-id port-id</b> parameter was introduced. |
| 10.07 or earlier | --                                                      |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-relay vsx active-active

```
dhcp-relay vsx active-active
no dhcp-relay vsx active-active
```

### Description

Enables DHCP relay active-active mode in VSX. When enabled, DHCP relay is active on both VSX Primary and Secondary peers. DHCP client requests are processed on the same VSX peer that receives them. A VSX peer that receives DHCP client request packets from its peer silently ignores them.

By default, this feature is disabled, and DHCP request packets are forwarded to the configured helper addresses only by the VSX primary.

The **no** form of this command disables DHCP relay active-active mode, and DHCP request packets are forwarded to configured helper addresses only by the VSX primary.

### Example

Enabling relay active-active mode in VSX.

```
switch(config)# dhcp-relay vsx active-active
```

Disabling relay active-active mode in VSX.

```
switch(config)# no dhcp-relay vsx active-active
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-smart-relay

```
dhcp-smart-relay
```

no dhcp-smart-relay

## Description

Enables DHCP Smart Relay on the device and on all the interfaces where IP helper addresses are configured. Disabled by default at the device level. Not supported on the management interface. The **no** form of this command disables DHCP Smart Relay.



Prior to enabling DHCP Smart Relay, enable IP helper address configuration and configure secondary IP addresses on the interface.

## Examples

Enabling DHCP Smart Relay:

```
switch(config)# dhcp-smart-relay
```

Disabling DHCP Smart Relay support:

```
switch(config)# no dhcp-smart-relay
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.10   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## diag-dump dhcp-relay basic

diag-dump dhcp-relay basic

## Description

Dumps DHCP relay configurations for all interfaces.

## Examples

This example enables DHCP relay support.

```
switch# diag-dump dhcp-relay basic
=====
```

[Start] Feature dhcp-relay Time : Sun Apr 26 06:38:10 2020

[Start] Daemon hpe-relay

DHCP Relay : 1  
DHCP Relay hop-count-increment : 1  
DHCP Relay Option82 : 1  
DHCP Relay Option82 validate : 0  
DHCP Relay Option82 policy : keep  
DHCP Relay Option82 remote-id : mac  
DHCP Relay Option82 Source Intf : Disable  
DHCP Smart Relay : Enable  
System Mac [f4:03:43:80:27:00]  
VRF :BLUE, Source Ip:200.0.0.10  
vsx: Not Present  
vsx: Present  
isl\_status: Up  
remote\_idl : 1  
VSX Active-Active Mode : Enable  
evpn VLANs: None  
evpn MAC clause : unset  
Allow IPv4 l2vpn client : enable

Interface vlan2: 1

Client Packet Statistics:

| Valid | Dropped | O82_Valid | O82_Dropped | vsx_drops |
|-------|---------|-----------|-------------|-----------|
| ----- | -----   | -----     | -----       | -----     |
| 0     | 0       | 0         | 0           | 0         |

Server Packet Statistics:

| Valid  | Dropped | O82_Valid | O82_Dropped | Invalid_IP_Drops | To_   |
|--------|---------|-----------|-------------|------------------|-------|
| Dsnoop | -----   | -----     | -----       | -----            | ----- |
| 0      | 0       | 0         | 0           | 0                | 0     |

client request dropped packets with extn option 82 = 0  
client request valid packets with extn option 82 = 0  
server request dropped packets with extn option 82 = 0  
server request valid packets with extn option 82 = 0  
Port 67 - 200.0.0.100,2  
source vrf-BLUE.

Interface vlan3: 1

Client Packet Statistics:

| Valid | Dropped | O82_Valid | O82_Dropped | vsx_drops |
|-------|---------|-----------|-------------|-----------|
| ----- | -----   | -----     | -----       | -----     |
| 0     | 0       | 0         | 0           | 0         |

Server Packet Statistics:

| Valid  | Dropped | O82_Valid | O82_Dropped | Invalid_IP_Drops | To_   |
|--------|---------|-----------|-------------|------------------|-------|
| Dsnoop | -----   | -----     | -----       | -----            | ----- |
| 0      | 0       | 0         | 0           | 0                | 0     |

client request dropped packets with extn option 82 = 0



```

client request valid packets with extn option 82 = 0
server request dropped packets with extn option 82 = 0
server request valid packets with extn option 82 = 0
Port 67 - 200.0.0.100,2
source vrf-BLUE.

DHCP Smart Relay Client Cache:
Total Number of entries: 2

Client-MAC PortIndex Timestamp RetryCount DiscCount GWIP

00:50:56:bd:6a:7a 20 1636105218 1 4 30.0.0.1
00:50:56:bd:71:17 20 1636105214 1 4 30.0.0.1

[End] Daemon hpe-relay

[End] Feature dhcp-relay
=====
Diagnostic-dump captured for feature dhcp-relay

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## ip bootp-gateway

```

ip bootp-gateway <IPv4-ADDR>
no ip bootp-gateway <IPv4-ADDR>

```

### Description

Configures a gateway address for the DHCP relay agent to use for DHCP requests. By default DHCP relay agent picks the lowest-numbered IP address on the interface.

The **no** form of this command removes the gateway address.

| Parameter   | Description                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------|
| <IPv4-ADDR> | Specifies the IP address of the gateway in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. |

## Examples

Setting the IP address of the gateway for interface 1/1/1 to **10.10.10.10**:

```
switch(config)# interface 1/1/1
switch(config-if)# ip bootp-gateway 10.10.10.10
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## ip helper-address

```
ip helper-address <IPv4-ADDR> [vrf <VRF-NAME>]
no ip helper-address <IPv4-ADDR> [vrf <VRF-NAME>]
```

### Description

Defines the address of a remote DHCP server or DHCP relay agent. Up to eight addresses can be defined. The DHCP relay agent forwards DHCP client requests to all defined servers.

If IP helper address is defined with VRF argument then this command requires you define a source IP address for DHCP relay with the command `ip source-interface`. The configured source IP on the VRF is used to forward DHCP packets to the server.

A helper address cannot be defined on the OOBM interface.

The **no** form of this command removes an IP helper address.

| Parameter                                     | Description                                                                                                          |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>helper-address &lt;IPv4-ADDR&gt;</code> | Specifies the helper IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. |
| <code>vrf &lt;VRF-NAME&gt;</code>             | Specifies the name of a VRF. Default: <b>default</b> .                                                               |

## Examples

Defining the IP helper address 10.10.10.209 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip helper-address 10.10.10.209
```

Removing the IP helper address 10.10.10.209 on interface 1/1/1:

```
switch(config-if)# no ip helper-address 10.10.10.209
```

Defining the IP helper address 10.10.10.209 on interface 1/1/2 on VRF myvrf:

```
switch(config)# interface 1/1/2
switch(config-if)# ip helper-address 10.10.10.209 vrf myvrf
```

Removing the IP helper address **10.10.10.209** on interface **1/1/2** on VRF **myvrf**:

```
switch(config-if)# no ip helper-address 10.10.10.209 vrf myvrf
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## show dhcp-relay

```
show dhcp-relay [vsx-peer]
```

### Description

Shows DHCP relay configuration settings.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

Showing DHCP relay settings:

```
switch# show dhcp-relay
```

```

DHCP Relay Agent : enabled
DHCP Request Hop Count Increment : enabled
L2VPN Clients : disabled
Option 82 : disabled
Source-Interface : disabled
Response Validation : disabled
Option 82 Handle Policy : replace
Remote ID : mac
DHCP Reply Overwrite Source IP : enabled
Option 82 Circuit ID Port-ID : enabled
VSX Active-Active Mode : enabled

```

#### DHCP Relay Statistics:

| Valid Requests | Dropped Requests | Valid Responses | Dropped Responses |
|----------------|------------------|-----------------|-------------------|
| 60             | 10               | 60              | 10                |

#### DHCP Relay Option 82 Statistics:

| Valid Requests | Dropped Requests | Valid Responses | Dropped Responses |
|----------------|------------------|-----------------|-------------------|
| 50             | 8                | 50              | 8                 |



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show dhcp-relay bootp-gateway

```
show dhcp-relay bootp-gateway [interface <INTERFACE-NAME>] [vsx-peer]
```

## Description

Shows the bootp gateway defined for all interfaces or a specific interface.

| Parameter        | Description                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-NAME> | Specifies an interface. Format: member/slot/port.                                                                                    |
| vsx-peer         | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the |

| Parameter | Description                                                                                 |
|-----------|---------------------------------------------------------------------------------------------|
|           | VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing the designated bootp gateway for all interfaces:

```
switch# show dhcp-relay bootp-gateway

BOOTP Gateway Entries

Interface Source IP

1/1/1 1.1.1.1
1/1/2 1.1.1.2
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ip helper-address

```
show ip helper-address [interface <INTERFACE-ID>] [vsx-peer]
```

## Description

Shows the IP helper addresses defined for all interfaces or a specific interface.

| Parameter                | Description                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface <INTERFACE-ID> | Specifies an interface. Format: member/slot/port.                                                                                                                                                                                |
| vsx-peer                 | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing the IP helper addresses for all interfaces:

```
switch# show ip helper-address
IP Helper Addresses

Interface: 1/1/1
IP Helper Address VRF

192.168.20.1 default
192.168.10.1 default

Interface: 1/1/2
IP Helper Address VRF

192.168.30.1 RED
```

Showing the IP helper addresses for interface 1/1/1:

```
switch# show ip helper-address interface 1/1/1
IP Helper Addresses

Interface: 1/1/1
IP Helper Address VRF

192.168.20.1 default
192.168.10.1 default
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## dhcpv6-relay

```
dhcpv6-relay [l2vpn-clients | source-interface]
no dhcpv6-relay [l2vpn-clients | source-interface]
```

### Description

Enables DHCPv6 relay support. DHCPv6 relay is disabled by default. DHCP relay is not supported on the management interface. Best practices is to disable this configuration on all the VXLAN tunnel endpoints (VTEPs), to avoid forwarding duplicate DHCPv6 requests to the server.

The **no** form of this command disables DHCP relay support.

DHCPv6 Relay requires that you configure the egress interface using the [ipv6 helper-address](#) command. The egress interface of a VTEP is used as an underlay, so a DHCPv6 Relay Multicast ipv6 address is not supported in a VXLAN topology.

| Parameter                     | Description                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------|
| <code>l2vpn-clients</code>    | Enables packets from l2vpn clients to be forwarded to configured servers. Enabled by default. |
| <code>source-interface</code> | Enables DHCPv6 relay to use the configured source interface.                                  |

### Usage

In Asymmetric/Symmetric Integrated Routing and Bridging (IRB) VXLAN deployments with a VLAN extension in subset of VTEPs, client DHCPv6 broadcast requests are received by all the VTEPs where a client VLAN is configured. A DHCPv6 relay agent on those VTEPs forward DHCPv6 packets to configured DHCPv6 server(s). As DHCPv6 requests are forwarded by multiple DHCPv6 relay agents, the DHCPv6 server receives duplicate copies of the same packet. When this configuration is disabled, the DHCPv6 relay agent on VTEPs ignores DHCPv6 request packets that are received from client MACs addresses learned via EVPN.

### Examples

Enables DHCPv6 relay support.

```
switch(config)# dhcpv6-relay
```

Removes DHCPv6 relay support.

```
switch(config)# no dhcpv6-relay
```



---

For more information on features that use this command, refer to the IP Services Guide for your switch model.

---

## Command History

| Release          | Modification                                            |
|------------------|---------------------------------------------------------|
| 10.12.1000       | <b>l2vpn-clients</b> and <b>source-interface</b> added. |
| 10.07 or earlier | --                                                      |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# dhcpv6-relay option 79

dhcpv6-relay option 79  
no dhcpv6-relay option 79

## Description

Enables support for DHCP relay option 79. When enabled, the DHCPv6 relay agent forwards the link-layer address of the client. This option is disabled by default.

The **no** form of this command disables support for DHCP relay option 79.

## Examples

Enables DHCP option 79 support.

```
switch(config)# dhcpv6-relay option 79
```

Disables DHCP option 79 support.

```
switch(config)# no dhcpv6-relay option 79
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |



# dhcpv6-relay vsx active-active

dhcpv6-relay vsx active-active  
no dhcpv6-relay vsx active-active

## Description

Enables DHCPv6 relay active-active mode in VSX. When enabled, DHCPv6 relay is active on both VSX Primary and Secondary peers. DHCPv6 client requests are processed on the same VSX peer that receives them. A VSX peer that receives DHCPv6 client request packets from its peer silently ignores them.

By default, this feature is disabled, and DHCPv6 request packets are forwarded to the configured helper addresses only by the VSX primary.

The **no** form of this command disables DHCPv6 relay active-active mode, and DHCPv6 request packets are forwarded to configured helper addresses only by the VSX primary.

## Example

Enabling relay active-active mode in VSX.

```
switch(config)# dhcpv6-relay vsx active-active
```

Disabling relay active-active mode in VSX.

```
switch(config)# no dhcpv6-relay vsx active-active
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config          | Administrators or local user group members with execution rights for this command. |

# diag-dump dhcpv6-relay basic

diag-dump dhcpv6-relay basic

## Description

Dumps DHCPv6 relay configurations for all interfaces.

## Examples

This example enables DHCP relay support.

```

switch# diag-dump dhcpv6-relay basic
=====
[Start] Feature dhcpv6-relay Time : Thu Jun 8 09:55:11 2017
=====

[Start] Daemon hpe-relay

DHCP Relay : 1
DHCPv6 Relay Option79 : 0
vsx: Present
vsx_status: Primary
isl_status: Up
VSX Active-Active Mode : Enable
evpn VLANs: None
evpn MAC clause : unset
Allow IPv6 l2vpn client : disable

System Mac [02:02:02:0a:0a]
Interface vlan10: 1
Intf selected IP - ifindex - 10 kernel ifindex - 1701::1, 1, egress = (null),
Server vrf = default

Client Packet Statistics:

Valid Dropped vsx_drops

0 0 0

Server Packet Statistics:

Valid Dropped To_Dsnoop

0 0 0

Total VRF source-ip entrie: 0

[End] Daemon hpe-relay

[End] Feature dhcpv6-relay
=====
Diagnostic-dump captured for feature dhcpv6-relay

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## ipv6 helper-address

```

ipv6 helper-address unicast <UNICAST-IPV6-ADDR>
no ipv6 helper-address unicast <UNICAST-IPV6-ADDR>
ipv6 helper-address multicast {all-dhcp-servers | <MULTICAST-IPV6-ADDR>} egress <PORT-
NUM>
no ipv6 helper-address multicast {all-dhcp-servers | <MULTICAST-IPV6-ADDR>} egress <PORT-
NUM>

```

### Description

Defines the address of a remote DHCPv6 server or DHCPv6 relay agent. Up to eight addresses can be defined. The DHCPv6 agent forwards DHCPv6 client requests to all defined servers.

Not supported on the OOBM interface.

The **no** form of this command removes an IP helper address.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <UNICAST-IPV6-ADDR>   | Specifies the unicast helper IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F.                                                                            |
| <MULTICAST-IPV6-ADDR> | Specifies the multicast helper IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F.                                                                          |
| all-dhcp-servers      | Specifies all the DHCP server IPv6 addresses for the interface.                                                                                                                                                                  |
| egress <PORT-NUM>     | Specifies the port number on which DHCPv6 service requests are relayed to a multicast destination. The egress port must be different than the one on which the multicast helper address is configured. Format: member/slot/port. |
| vrf <VRF-NAME>        | Specifies the name of the VRF from which the specified protocol sets its source IP address.                                                                                                                                      |

### Examples

Defining a multicast IPv6 helper address of **2001:DB8::1** on port **1/1/2**:

```
switch(config-if)# ipv6 helper-address multicast 2001:DB8:0:0:0:0:0:1 egress 1/1/2
```

Removing the IP helper address of **2001:DB8::1** on port **1/1/2**:

```
switch(config-if)# no ipv6 helper-address multicast 2001:DB8:0:0:0:0:0:1 egress 1/1/2
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## show dhcpv6-relay

show dhcpv6-relay [vsx-peer]

### Description

Shows DHCP relay configuration settings.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

```
switch(config)# show dhcpv6-relay
DHCPv6 Relay Agent : enabled
Option 79 : disabled
L2vpn-clients : enabled
Source-interface : enabled
VSX Active-Active Mode : enabled
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ipv6 helper-address

show ipv6 helper-address [interface <INTERFACE-ID>] [vsx-peer]

## Description

Shows the helper IP addresses defined for all interfaces or a specific interface.

| Parameter                | Description                                                                                                                                                                                                                      |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface <INTERFACE-ID> | Specifies an interface. Format: <b>member/slot/port</b> .                                                                                                                                                                        |
| vsx-peer                 | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

```
switch# show ipv6 helper-address
```

```
Interface: 1/1/1
IPv6 Helper Address Egress Port

2001:db8:0:1:: -
FF01::1:1000 1/1/2
```

```
Interface: 1/1/2
IPv6 Helper Address Egress Port

2001:db8:0:1:: -
```

```
switch# show ipv6 helper-address interface 1/1/1
```

```
Interface: 1/1/1
IPv6 Helper Address Egress Port

2001:db8:0:1:: -
FF01::1:1000 1/1/2
```

```
switch# show ipv6 helper-address interface vlan20
```

```
Interface: vlan20
IP Helper Address Egress Port

2001::1 -
ff01::1:1000 vlan30 default
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## authoritative

authoritative  
no authoritative

### Description

Configures the DHCPv4 server as *authoritative* on the current VRF. This means that the server is the sole authority for the network on the VRF. Therefore, if a client requests an IP address lease for which the server has no record, the server responds with DHCPNAK, indicating that the client must no longer use that IP address. If the server is not authoritative, then it will ignore DHCPv4 requests received for unknown leases from unknown hosts.

The **no** form of this command disables authoritative mode on the current VRF.

### Example

Configures DHCPv4 server authoritative mode on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# authoritative
```

Removes the DHCPv4 server authoritative mode on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# no authoritative
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context    | Authority                                                                          |
|---------------|--------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

## bootp

```
bootp <REMOTE-URL>
no bootp <REMOTE-URL>
```

## Description

Sets the BOOTP options that are returned by the DHCPv4 server for the current pool. BOOTP provides a way to distribute an IP address and boot image file to client stations. The DHCPv4 server returns the IP address and the location of the boot image file, which must be stored on an external TFTP server.

The **no** form of this command disables support for BOOTP.

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;REMOTE-URL&gt;</code> | <p>Specifies the name and location of a BOOTP file on a TFTP server in the format:</p> <pre>tftp://{&lt;IP&gt;   &lt;HOST&gt;}/&lt;FILE&gt;</pre> <ul style="list-style-type: none"><li>▪ <b>&lt;IP&gt;</b>: Specifies the IP address of the TFTP server hosting the file in IPv4 format (<b>x.x.x.x</b>), where <b>x</b> is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100.</li><li>▪ <b>&lt;HOST&gt;</b>: Specifies the fully-qualified domain name of the TFTP server hosting the file. Range: 1 to 64 printable ASCII characters.</li><li>▪ <b>&lt;FILE&gt;</b>: Specifies the name of the BOOTP file. Range: 1 to 64 printable ASCII characters.</li></ul> |

## Example

Defines BOOTP support on the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# bootp tftp://10.0.0.1/mybootfile
```

Deletes BOOTP support on the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no bootp tftp://10.0.0.1/mybootfile
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information



| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## clear dhcp-server leases

```
clear dhcp-server leases [all-vrfs | <IPv4-ADDR> vrf <VRF-NAME>] | vrf <VRF-NAME>]
```

### Description

Clears DHCPv4 server lease information. The DHCPv4 server must be disabled before clearing lease information.

| Parameter                  | Description                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all-vrfs                   | Clears leases for all VRFs.                                                                                                                                                                                                                                             |
| <IPv4-ADDR> vrf <VRF-NAME> | Clears the lease for a specific client on a specific VRF. Specify the client address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100. |
| vrf <VRF-NAME>             | Clears leases for a specific VRF.                                                                                                                                                                                                                                       |

### Examples

Clearing all DHCPv4 server leases.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
switch(config-dhcp-server)# exit
switch(config)# exit
switch# clear dhcp-server leases
```

Clearing all DHCPv4 server leases for VRF **primary-vrf**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
switch(config-dhcp-server)# exit
switch(config)# exit
switch# clear dhcp-server leases vrf primary-vrf
```

Clear the DHCPv4 server lease for IP address **10.10.10.1** on VRF **primary-vrf**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
switch(config-dhcp-server)# exit
switch(config)# exit
switch# clear dhcp-server leases 10.10.10.1 vrf primary-vrf
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## default-router

```
default-router <IPv4-ADDR-LIST>
no default-router <IPv4-ADDR-LIST>
```

### Description

Defines up to four default routers for the current DHCPv4 server pool.

The **no** form of this command removes the specified default routers from the pool.

| Parameter        | Description                                                                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv4-ADDR-LIST> | Specifies the IP addresses of the default routers in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100. Separate addresses with a space. A maximum of four IP addresses can be defined. |

### Example

Defines two default routers, **10.0.0.1** and **10.0.0.10**, for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# default-router ip 10.0.0.1 10.0.0.10
```

Deletes the default router **10.0.0.1** from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no default-router ip 10.0.0.1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## dhcp-server external-storage

```
dhcp-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
no dhcp-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
```

### Description

Configures the external storage file location for DHCPv4 server lease information. This file provides persistent storage, enabling DHCPv4 server settings to be restored when the switch is restarted. Lease information is stored in a flat file on the configured external device.

If external storage is not configured, then after a failure or reboot, all existing lease information is lost. Lease information is saved to external storage each time the delay timer expires, which by default is every 300 seconds.

Lease information is not restored when issuing the command `dhcp-server enable`.

The **no** form of this command removes external storage support for the DHCPv4 server.

| Parameter                                | Description                                                                                                       |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <code>&lt;VOLUME-NAME&gt;</code>         | Specifies the external storage volume name. Range: 1 to 64 printable ASCII characters.                            |
| <code>file &lt;LEASE-FILENAME&gt;</code> | Specifies the external storage filename. Range: 1 to 255 printable ASCII characters.                              |
| <code>delay &lt;DELAY&gt;</code>         | Specifies the interval in seconds between updates to the external storage file. Range: 15 to 86400. Default: 300. |

### Example

Stores the lease file on external storage volume **Storage1** in file **LeaseFile** at an interval of 600 seconds.

```
switch(config)# dhcp-server external-storage Storage1 file LeaseFile delay 600
```

Disables storage of the lease file on external storage volume **Storage1** in file **LeaseFile**.

```
switch(config)# no dhcp-server external-storage Storage1 file LeaseFile delay 600
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## dhcp-server vrf

```
dhcp-server vrf <VRF-NAME>
no dhcp-server vrf <VRF-NAME>
```

### Description

Configures the DHCPv4 server to support a VRF and changes to the `config-dhcp-server` context for that VRF.

The **no** form of this command removes DHCPv4 server support on a VRF.

| Parameter  | Description    |
|------------|----------------|
| <VRF-NAME> | Name of a VRF. |

### Example

Configures DHCPv4 server support on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
```

Removes DHCPv4 server support on VRF **primary**.

```
switch(config)# no dhcp-server vrf primary
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## disable

disable

### Description

Disables the DHCPv4 server on the current VRF. The DHCPv4 server is disabled by default when configured on a VRF.

### Example

Disables the DHCPv4 server on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# disable
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context    | Authority                                                                          |
|---------------|--------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

## dns-server

```
dns-server <IPv4-ADDR-LIST>
no dns-server <IPv4-ADDR-LIST>
```

### Description

Defines up to four DNS servers for the current DHCPv4 server pool.

The **no** form of this command removes the specified DNS servers from the pool.

| Parameter        | Description                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv4-ADDR-LIST> | Specifies the IP addresses of the DNS servers in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. Separate addresses with a space. |

## Example

Defines DNS servers for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# dns-server 10.0.20.1
```

Deletes a DNS server from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no dns-server 10.0.20.1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## domain-name

domain-name <DOMAIN-NAME>  
no domain-name <DOMAIN-NAME>

## Description

Defines a domain name for the current DHCPv4 server pool.

The **no** form of this command removes the specified domain name from the pool.

| Parameter     | Description                                                          |
|---------------|----------------------------------------------------------------------|
| <DOMAIN-NAME> | Specifies a domain name. Range: 1 to 255 printable ASCII characters. |

## Example

Defines a domain name for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# domain-name example.org.in
```

Deletes a domain name from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no domain-name example.org.in
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## enable

enable

### Description

Enables the DHCPv4 server on the current VRF. The DHCPv4 server is disabled by default when configured on a VRF.

### Example

Enables the DHCPv4 server on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# enable
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context    | Authority                                                                          |
|---------------|--------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

## lease

```
lease {<TIME> | infinite}
no lease
```

### Description

Sets the length of the DHCPv4 lease time for the current pool. The lease time determines how long an IP address is valid before a DHCPv4 client must request that it be renewed.

The **no** form of this command returns the DHCPv4 lease time to its default value 1 hour.

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| <TIME>    | Sets the DHCPv4 lease time. Format: DD:HH:MM. Default: 01:00:00.                             |
| infinite  | Sets the DHCPv4 lease time to infinite. This means that addresses do not need to be renewed. |

### Example

Sets the lease time for DHCPv4 server pool **primary-pool** on VRF **primary** to **12** hours.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# lease 00:12:00
```

Deletes the lease time for DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no lease 00:12:00
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information



| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## netbios-name-server

```
netbios-name-server <IPV4-ADDR-LIST>
no netbios-name-server <IPV4-ADDR-LIST>
```

### Description

Defines up to four NetBIOS WINS servers for the current DHCPv4 server pool. WINS is used by Microsoft DHCP clients to match host names with IP addresses.

The **no** form of this command removes the specified WINS servers from the pool.

| Parameter                     | Description                                                                                                                                                                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;IPV4-ADDR-LIST&gt;</i> | Specifies the IP addresses of NetBIOS (WINS) servers in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. Separate addresses with a space. A maximum of four IP addresses can be defined. |

### Example

Defines two WINS servers for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# netbios-name-server ip 10.0.20.1 10.0.30.10
```

Deletes a WINS server from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no netbios-name-server ip 10.0.20.1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

# netbios-node-type

netbios-node-type <TYPE>  
no netbios-node-type <TYPE>

## Description

Defines the NetBIOS node type for the current DHCPv4 server pool.

The **no** form of this command removes the NetBIOS node type for the current pool.

| Parameter | Description                                                                 |
|-----------|-----------------------------------------------------------------------------|
| <TYPE>    | Specifies the NetBIOS node type: broadcast, hybrid, mixed, or peer-to-peer. |

## Examples

Defines the NetBIOS node type **broadcast** for the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# netbios-node-type broadcast
```

Deletes the NetBIOS node type **broadcast** from the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no netbios-node-type broadcast
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

# option

option <OPTION-NUM> {ascii "<ASCII-STR>" | hex <HEX-STR> | ip <IPV4-ADDR-LIST>}  
no option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPV4-ADDR-LIST>}

## Description

Defines custom DHCPv4 options for the current DHCPv4 server pool. DHCPv4 options enable the DHCPv4 server to provide additional information about the network when DHCPv4 clients request an address.

The **no** form of this command removes custom DHCPv4 options from the pool.

| Parameter                              | Description                                                                                                                                                                                                                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;OPTION-NUM&gt;</code>        | Specifies a DHCPv4 option number. For a list of DHCPv4 option numbers, see <a href="https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml">https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml</a> . Range: 2 to 254. |
| <code>ascii &lt;ASCII-STR&gt;</code>   | <p>Specifies a value for the selected option as an ASCII string. Range: 1 to 255 ASCII characters.</p> <p><b>NOTE:</b> If you specify <b>18</b> as the <code>&lt;OPTION-NUM&gt;</code> parameter, the ASCII string must be enclosed within quotation marks ("").</p>              |
| <code>hex &lt;HEX-STR&gt;</code>       | Specifies a value for the selected option as a hexadecimal string. Range: 1 to 255 hexadecimal characters.                                                                                                                                                                        |
| <code>ip &lt;IPV4-ADDR-LIST&gt;</code> | Specifies a list of IP addresses in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. Separate addresses with a space. A maximum of four IP addresses can be defined.                                                                             |

## Example

Defines DHCPv4 option **3** for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# option 3 ip 192.168.1.1
```

Deletes DHCPv4 option **3** for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no option 3 ip 192.168.1.1
```

Defines DHCPv4 option 18 for the server pool **mgmt-test** on VRF **mgmt**.

```
switch(config)# dhcp-server vrf mgmt
switch(config-dhcp-server)# pool mgmt-test
switch(config-dhcp-server-pool)# option 18 ascii "aswed"
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## pool

```
pool <POOL-NAME>
no pool <POOL-NAME>
```

### Description

Creates a DHCPv4 server pool for the current VRF and switches to the `config-dhcp-server-pool` context for it. Multiple pools, each with a distinct range, can be assigned to a VRF. A maximum of 64 pools (IPv4 and IPv6), 64 address ranges, and 8182 clients are supported on the switch across all VRFs. The **no** form of this command deletes the specified DHCPv4 server pool.

| Parameter   | Description                                                                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POOL-NAME> | Specifies the DHCPv4 pool name. A maximum of 64 pools (IPv4 and IPv6) are supported across VRFs on the switch. Range: 1 to 32 printable ASCII characters. First character must be a letter or number. |

### Example

Creates the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)#
```

Deletes the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# no pool primary-pool
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context    | Authority                                                                          |
|---------------|--------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server | Administrators or local user group members with execution rights for this command. |

## range

```
range <LOW-IPV4-ADDR> <HIGH-IPV4-ADDR> [prefix-len <MASK>]
no range <LOW-IPV4-ADDR> <HIGH-IPV4-ADDR> [prefix-len <MASK>]
```

### Description

Defines the range of IP addresses supported by the current DHCPv4 server pool. A maximum of 64 ranges are supported per switch across all VRFs.

The **no** form of this command deletes the address range for the current pool.

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LOW-IPV4-ADDR>   | Specifies the lowest IP address in the pool in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <HIGH-IPV4-ADDR>  | Specifies the highest IP address in the pool in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| prefix-len <MASK> | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 32.<br><br><b>NOTE:</b> When active gateway is configured on the interface serviced by the pool, you must specify a prefix length that matches the mask on the IP address assigned to the interface. Otherwise, client stations will get a prefix length from active gateway that may not be consistent with the configured range, and a DHCP error will occur. In the following example, the DHCP range prefix is set to 16 to match the mask on the IP address assigned to interface VLAN 2.<br><br><pre>switch(config)# interface vlan 2 switch(config-if-vlan)# ip address 200.1.1.1/16 switch(config-if-vlan)# active-gateway ip 200.1.1.3 mac 00:aa:aa:aa:aa:aa switch(config-if-vlan)# exit switch(config)# dhcp-server vrf primary switch(config-dhcp-server)# pool primary-pool switch(config-dhcp-server-pool)# range 192.168.1.1 192.168.1.100 prefix-len 16</pre> |

### Examples

Defines the address range **192.168.1.1** to **192.168.1.100** with a mask of **24** bits for the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# 192.168.1.1 192.168.1.100 prefix-len 24
```

Deletes the address range **192.168.1.1** to **192.168.1.100** with a mask of **24** bits from the DHCPv4 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no 192.168.1.1 192.168.1.100 prefix-len 24
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## show dhcp-server

```
show dhcp-server [all-vrfs]
show dhcp-server leases {all-vrfs | vrf <VRF-NAME>}
show dhcp-server pool <POOL-NAME> [vrf <VRF-NAME>]
```

## Description

Shows configuration settings for the DHCPv4 server.

| Parameter                          | Description                                                                      |
|------------------------------------|----------------------------------------------------------------------------------|
| all-vrfs                           | Shows DHCPv4 server configuration settings for all VRFs.                         |
| leases {all-vrfs   vrf <VRF-NAME>} | Shows DHCPv4 server lease provided by the server for all VRFs or a specific VRF. |
| pool <POOL-NAME> [vrf <VRF-NAME>]  | Shows DHCPv4 server pool configuration settings for all VRFs or a specific VRF.  |

## Examples

Showing all DHCPv4 server configuration settings.

```
switch# show dhcp-server

VRF Name : default
DHCP Server : enabled
Operational State : operational
Authoritative Mode : false
Config_status : Applied

Pool Name : test
```

Lease Duration : 00:01:00

DHCP dynamic IP allocation

| Start-IP-Address | End-IP-Address | Prefix-Length |
|------------------|----------------|---------------|
| 192.168.1.1      | 192.168.1.20   | 24            |

DHCP Server options

| Option-Number | Option-Type | Option-Value                        |
|---------------|-------------|-------------------------------------|
| 6             | ip          | 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.6 |

DHCP Server static IP allocation

| IP-Address | Client-Hostname | State       | MAC-Address       |
|------------|-----------------|-------------|-------------------|
| 10.0.0.3   | *               | OPERATIONAL | aa:aa:aa:aa:aa:aa |

BOOTP Options

| Boot-File-Name | TFTP-Server-Name | TFTP-Server-Address |
|----------------|------------------|---------------------|
| boot.txt       | *                | 10.0.0.10           |

Showing DHCP server configuration settings for VRF **primary-vrf**.

switch# **show dhcp-server vrf primary-vrf**

VRF Name : primary-vrf  
DHCP Server : disabled  
Operational State : disabled  
Authoritative Mode : false  
Config\_status : Applied

Pool Name : test  
Lease Duration : 00:01:00

DHCP dynamic IP allocation

| Start-IP-Address | End-IP-Address | Prefix-Length |
|------------------|----------------|---------------|
| 10.0.0.1         | 10.0.0.30      | *             |
| 192.168.1.1      | 192.168.1.20   | 24            |
| 192.168.10.30    | 192.168.10.60  | 16            |

DHCP Server options

| Option-Number | Option-Type | Option-Value                        |
|---------------|-------------|-------------------------------------|
| 6             | ip          | 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.6 |
| 18            | ascii       | aswed                               |

DHCP Server static IP allocation

```

IP-Address Client-Hostname MAC-Address

10.0.0.1 * aa:bb:cc:11:12:a4
20.0.0.1 * 11:22:11:22:aa:dd

```

#### BOOTP Options

```

Boot-File-Name TFTP-Server-Name State TFTP-Server-Address

boot.txt * OPERATIONAL 10.0.0.10

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## static-bind

```

static-bind {ip <IPV4-ADDR>}|{ mac <MAC-ADDR>} [hostname <HOST>]
no static-bind <IPV4-ADDR-LIST>

```

## Description

Creates a static binding that associates an IP address in the current pool with a specific MAC address. This causes the DHCPv4 server to only assign the specified IP address to a client station with the specified MAC address.

The **no** form of this command removes the specified binding.

| Parameter       | Description                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPV4-ADDR>     | Specifies an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. The IP address must be within the address range defined for the current pool. |
| mac <MAC-ADDR>  | Specifies a client station MAC address ( <b>xx:xx:xx:xx:xx:xx</b> ), where <b>x</b> is a hexadecimal number from 0 to F.                                                                   |
| hostname <HOST> | Specifies the host name of the client station. Range: 1 to 255 printable ASCII characters                                                                                                  |



Examples

Defines a static address for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# static-bind ip 10.0.0.1 mac 24:be:05:24:75:73
```

Deletes a static address from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcp-server vrf primary
switch(config-dhcp-server)# pool primary-pool
switch(config-dhcp-server-pool)# no static-bind ip 10.0.0.1 mac 24:be:05:24:75:73
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcp-server-pool | Administrators or local user group members with execution rights for this command. |

## authoritative

authoritative  
no authoritative

### Description

Configures the DHCPv6 server as *authoritative* on the current VRF. This means that the server is the sole authority for the network on the VRF. It responds to client solicit messages with advertise messages having a priority/preference value set to 255 (the maximum), instead of 0 (the minimum). Clients always choose the DHCPv6 server with the highest priority/preference value. If two DHCPv6 servers send an advertise message with the same priority/preference value, then the client picks one and discards the other.

The **no** form of this command disables authoritative mode on the current VRF.

### Example

Configures DHCPv6 server authoritative mode on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# authoritative
```

Removes DHCPv6 server authoritative mode on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# no authoritative
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context      | Authority                                                                          |
|---------------|----------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

# clear dhcpv6-server leases

```
clear dhcpv6-server leases [all-vrfs | <IPv6-ADDR> vrf <VRF-NAME>] | vrf <VRF-NAME>]
```

## Description

Clears DHCPv6 server lease information. The DHCPv6 server must be disabled before clearing lease information.

| Parameter                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all-vrfs                   | Clears leases for all VRFs.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <IPv6-ADDR> vrf <VRF-NAME> | Clears the lease for a specific client on a specific VRF. Specify the client address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. You can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address<br>2222:0000:3333:0000:0000:0000:4444:0055 becomes<br>2222:0:3333::4444:55. |
| vrf <VRF-NAME>             | Clears leases for a specific VRF.                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Examples

Clearing all DHCPv6 server leases.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
switch(config-dhcpv6-server)# exit
switch(config)# exit
switch# clear dhcpv6-server leases
```

Clearing all DHCPv6 server leases for VRF **primary-vrf**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
switch(config-dhcpv6-server)# exit
switch(config)# exit
switch# clear dhcpv6-server leases vrf primary-vrf
```

Clear the DHCPv6 server lease for IP address **2001::1** on VRF **primary-vrf**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
switch(config-dhcpv6-server)# exit
switch(config)# exit
switch# clear dhcpv6-server leases 2001::1 vrf primary-vrf
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## dhcpv6-server external-storage

```
dhcpv6-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
no dhcpv6-server external-storage <VOLUME-NAME> file <LEASE-FILENAME> [delay <DELAY>]
```

### Description

Configures the external storage file location for DHCPv6 server lease information. This file provides persistent storage, enabling DHCPv6 server settings to be restored when the switch is restarted. Lease information is stored in a flat file on the configured external device.

If external storage is not configured, then after a failure or reboot, all existing lease information is lost. Lease information is saved to external storage each time the delay timer expires, which by default is every 300 seconds.

Lease information is not restored when issuing the command **dhcp-server enable**.

The **no** form of this command removes external storage support for the DHCPv6 server.

| Parameter             | Description                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------|
| <VOLUME-NAME>         | Specifies the external storage volume name. Range: 1 to 64 printable ASCII characters.                            |
| file <LEASE-FILENAME> | Specifies the external storage filename. Range: 1 to 255 printable ASCII characters.                              |
| delay <DELAY>         | Specifies the interval in seconds between updates to the external storage file. Range: 15 to 86400. Default: 300. |

### Example

Stores the lease file on external storage volume **Storage1** in file **LeaseFile** at an interval of 600 seconds.

```
switch(config)# dhcpv6-server external-storage Storage1 file LeaseFile delay 600
```

Disables storage of the lease file on external storage volume **Storage1** in file **LeaseFile**.

```
switch(config)# no dhcpv6-server external-storage Storage1 file LeaseFile delay 600
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## dhcpv6-server vrf

```
dhcpv6-server vrf VRF-NAME
no dhcpv6-server vrf VRF-NAME
```

### Description

Configures the DHCPv6 server to support a VRF and changes to the **config-dhcpv6-server** context for that VRF.

The **no** form of this command removes DHCPv6 server support on a VRF.

| Parameter       | Description    |
|-----------------|----------------|
| <i>VRF-NAME</i> | Name of a VRF. |

### Example

Configures DHCPv6 server support on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
```

Removes the DHCPv6 server support on VRF **primary**.

```
switch(config)# no dhcpv6-server vrf primary
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## disable

disable

### Description

Disables the DHCPv6 server on the current VRF. The DHCPv6 server is disabled by default when configured on a VRF.

### Example

Disables the DHCPv6 server on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# disable
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context      | Authority                                                                          |
|---------------|----------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## dns-server

```
dns-server <IPv6-ADDR-LIST>
no dns-server <IPv6-ADDR-LIST>
```

### Description

Defines up to four DNS servers for the current DHCPv6 server pool.

The **no** form of this command removes the specified DNS servers from the pool.

| Parameter                     | Description                                                                                                                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;IPv6-ADDR-LIST&gt;</i> | Specifies the IP addresses of the DNS servers in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. Separate addresses with a space. A maximum of four IP addresses can be defined. |

## Example

Defines DNS server **2001::13** for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# dns-server 2001::13
```

Deletes DNS server **2001::13** from the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no dns-server 2001::13
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## enable

enable

## Description

Enables the DHCPv6 server on the current VRF. The DHCPv6 server is disabled by default when configured on a VRF.

## Example

Enables the DHCPv6 server on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# enable
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context      | Authority                                                                          |
|---------------|----------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## lease

```
lease {<TIME> | infinite}
no lease
```

## Description

Sets the length of the DHCPv6 lease time for the current pool. The lease time determines how long an IP address is valid before a DHCPv6 client must request that it be renewed.

The **no** form of this command returns the DHCPv6 lease time to the default value 1 hour.

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| <TIME>    | Sets the DHCPv6 lease time. Format: DD:HH:MM. Default: 01:00:00.                             |
| infinite  | Sets the DHCPv6 lease time to infinite. This means that addresses do not need to be renewed. |

## Example

Sets the lease time for DHCPv6 server pool **primary-pool** on VRF **primary** to **12** hours.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# lease 00:12:00
```

Sets the lease time for DHCP server pool **primary-pool** on VRF **primary** to the default value.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no lease 00:12:00
```





For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## option

option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPv6-ADDR-LIST>}  
no option <OPTION-NUM> {ascii <ASCII-STR> | hex <HEX-STR> | ip <IPv6-ADDR-LIST>}

## Description

Defines custom DHCPv6 options for the current DHCPv6 server pool.

The **no** form of this command removes custom DHCPv6 options from the pool.

| Parameter           | Description                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <OPTION-NUM>        | Specifies a DHCPv6 option number. Range: 2 to 254.                                                                                                     |
| ascii <ASCII-STR>   | Specifies a value for the selected option as an ASCII string. Range: 1 to 255 ASCII characters.                                                        |
| hex <HEX-STR>       | Specifies a value for the selected option as a hexadecimal string. Range: 1 to 255 hexadecimal characters.                                             |
| ip <IPv6-ADDR-LIST> | Specifies a list of IP addresses for the option in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. |

## Example

Defines DHCPv6 option **22** for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# option 22 ipv6 2001::12
```

Deletes DHCPv6 option 22 for the server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no option 22 ipv6 2001::12
```

Defines DHCPv6 option **18** for the server pool **mgmt-test** on VRF **mgmt**.

```
switch(config)# dhcpv6-server vrf mgmt
switch(config-dhcpv6-server)# pool mgmt-test
switch(config-dhcpv6-server-pool)# option 18 ascii "aswed"
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## pool

```
pool <POOL-NAME>
no pool <POOL-NAME>
```

## Description

Creates a DHCPv6 server pool for the current VRF and switches to the `config-dhcpv6-server-pool` context for it. Multiple pools, each with a distinct range, can be assigned to a VRF. A maximum of 64 pools (IPv4 and IPv6), 64 address ranges, and 8182 clients are supported on the switch across all VRFs. The **no** form of this command deletes the specified DHCPv6 server pool.

| Parameter   | Description                                                                                                                                                                                           |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <POOL-NAME> | Specifies the DHCPv6 pool name. A maximum of 64 pools (IPv4 and IPv6) are supported across VRFs on the switch. Range: 1 to 32 printable ASCII characters. First character must be a letter or number. |

## Example

Creates the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)#
```

Deletes the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# no pool primary-pool
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context      | Authority                                                                          |
|---------------|----------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server | Administrators or local user group members with execution rights for this command. |

## range

```
range <LOW-IPV6-ADDR> <HIGH-IPV6-ADDR> [prefix-len <MASK>]
no range <LOW-IPV6-ADDR> <HIGH-IPV6-ADDR> [prefix-len <MASK>]
```

## Description

Defines the range of IP addresses supported by the current DHCPv6 server pool. A maximum of 64 ranges are supported per switch across all VRFs.

The **no** form of this command deletes the address range for the current pool.

| Parameter         | Description                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LOW-IPV6-ADDR>   | Specifies the lowest IP address in the pool in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F.  |
| <HIGH-IPV6-ADDR>  | Specifies the highest IP address in the pool in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. |
| prefix-len <MASK> | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 64 to 128.                           |

## Example

Defines an address range for the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# range 2001::1 2001::10 prefix-len 64
```

Deletes an address range for the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no range 2001::1 2001::10 prefix-len 64
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## show dhcpv6-server

```
show dhcpv6-server [all-vrfs]
show dhcpv6-server leases {all-vrfs | vrf <VRF-NAME>}
show dhcpv6-server pool <POOL-NAME> [vrf <VRF-NAME>]
```

## Description

Shows configuration settings for the DHCPv6 server.

| Parameter                          | Description                                                                      |
|------------------------------------|----------------------------------------------------------------------------------|
| all-vrfs                           | Shows DHCPv6 server configuration settings for all VRFs.                         |
| leases {all-vrfs   vrf <VRF-NAME>} | Shows DHCPv6 server lease provided by the server for all VRFs or a specific VRF. |
| pool <POOL-NAME> [vrf <VRF-NAME>]  | Shows DHCPv6 server pool configuration settings for all VRFs or a specific VRF.  |

## Examples

Showing all DHCPv6 server configuration settings.

```

switch# show dhcpv6-server

VRF Name : default
DHCPv6 Server : enabled
Operational State : operational
Authoritative Mode : true
Config_status : Applied

Pool Name : test
Lease Duration : 00:01:00

DHCPV6 dynamic IP allocation

Start-IPv6-Address End-IPv6-Address Prefix-Length

2001::2 2001::10 64

DHCPv6 Server options

Option-Number Option-Type Option-Value

7 ipv6 2001::15

DHCPv6 Server static IP allocation

DHCPv6 Server static host is not configured.

```

Showing DHCPv6 server configuration settings for VRF **primary-vrf**.

```

switch# show dhcpv6-server vrf primary-vrf

VRF Name : primary-vrf
DHCPv6 Server : disabled
Operational State : standby
Authoritative Mode : false
Config_status : Applied

Pool Name : test
Lease Duration : 00:01:00

DHCPV6 dynamic IP allocation

Start-IPv6-Address End-IPv6-Address Prefix-Length

2000::1 2000::20 *
2001::20 2001::50 *
2001::2 2001::10 64
2010::20 2010::40 *

DHCPv6 Server options

Option-Number Option-Type Option-Value

7 ipv6 2001::15
23 ipv6 2001::30
30 ipv6 2001::10

DHCPv6 Server static IP allocation

```

```
DHCPv6 Server static host is not configured.
```

```
Pool Name : v6test
Lease Duration : 00:01:00
```

```
DHCPv6 dynamic IP allocation
```

| Start-IPv6-Address | End-IPv6-Address | Prefix-Length |
|--------------------|------------------|---------------|
| 2001::1            | 2001::20         | 64            |
| 2010::10           | 2010::30         | *             |
| 2020::20           | 2020::60         | *             |

```
DHCPv6 Server options
```

| Option-Number                           | Option-Type | Option-Value                            |
|-----------------------------------------|-------------|-----------------------------------------|
| 7                                       | ipv6        | 2001::20                                |
| 23                                      | ipv6        | 2001:0db8:85a3:0000:0000:8a2e:0370:7334 |
| 2001:0db8:85a3:0000:0000:8a2e:0370:7335 |             |                                         |
| 2001:0db8:85a3:0000:0000:8a2e:0370:7336 |             |                                         |
| 2001:0db8:85a3:0000:0000:8a2e:0370:7337 |             |                                         |

```
DHCPv6 Server static IP allocation
```

| IPv6-Address | Client-Hostname | State       | Client-Id          |
|--------------|-----------------|-------------|--------------------|
| 2100::4      | *               | OPERATIONAL | 1:0:a0:24:ab:fb:9c |



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## static-bind

```
static-bind ipv6 <IPVv6-ADDR> client-id <ID> [hostname <HOST>]
no static-bind ipv6 <IPVv6-ADDR-LIST>
```

## Description

Creates a static binding that associates an IP address in the current pool with a client identifier or DUID. This causes the DHCPv6 server to only assign the specified IP address to a client station with the specified client identifier or DUID.

The **no** form of this command removes the specified static binding from the pool.

| Parameter                          | Description                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;IPv6-ADDR&gt;</code>     | Specifies the IP address to assign in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55. |
| <code>client-id &lt;ID&gt;</code>  | Specifies the client identifier or DUID.                                                                                                                                                                                                         |
| <code>hostname &lt;HOST&gt;</code> | Specifies the host name of the client station. Range: 1 to 255 printable ASCII characters                                                                                                                                                        |

## Example

Defines a static address for the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# static-bind ipv6 2001::10 client-id
1:0:a0:24:ab:fb:9c
```

Deletes a static address from the DHCPv6 server pool **primary-pool** on VRF **primary**.

```
switch(config)# dhcpv6-server vrf primary
switch(config-dhcpv6-server)# pool primary-pool
switch(config-dhcpv6-server-pool)# no static-bind ipv6 2001::10 client-id
1:0:a0:24:ab:fb:9c
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-dhcpv6-server-pool | Administrators or local user group members with execution rights for this command. |

## http-proxy

```
http-proxy {<FQDN | IPV4-ADDR> | IPV6-ADDR[:PORT]} [vrf <VRF-NAME>]
no http-proxy [<FQDN | IPV4-ADDR>] [vrf <VRF-NAME>]
```

### Description

Specifies HTTP proxy location and VRF.

When HTTP proxy location and VRF are configured on the switch, it overrides any existing HTTP proxy location and VRF as this has the highest priority over the values obtained from other sources.

Following locations can be used for the HTTP proxy location:

- A fully qualified domain name (FQDN).
- An IPv4 address with colon separated port number
- An IPv6 address with colon separated port number



When configuring an IPv6 address with a port number, the address must be specified inside square brackets. An example - [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:8080.

If the command is entered without the VRF parameter, then the VRF used will be 'default' VRF.

The **no** form of this command removes a specified HTTP proxy location.

| Parameter   | Description                                     |
|-------------|-------------------------------------------------|
| <FQDN>      | Specifies FQDN for HTTP proxy location.         |
| <IPV4-ADDR> | Specifies IPV4 address for HTTP proxy location. |
| <IPV6-ADDR> | Specifies IPV6 address for HTTP proxy location. |
| <VRF-NAME>  | Specifies VRF for HTTP proxy.                   |



A FQDN or IPV4 address are optional in the **no** form of the command.

### Examples

Specifying a FQDN for HTTP proxy location and **MGMT** VRF with an IPv6 address:

```
switch(config)# http-proxy http-proxy.example.com vrf mgmt
switch(config)# http-proxy [2000::100]:8080 vrf mgmt
```



Specifying a FQDN for HTTP proxy location and **MGMT** VRF with an IPv4 address:

```
switch(config)# http-proxy http-proxy.example.com vrf mgmt
switch(config)# http-proxy 192.168.1.3:8080 vrf mgmt
```

Removing HTTP proxy location

```
switch(config)# no http-proxy
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification                             |
|------------------|------------------------------------------|
| 10.13.1000       | Command updated to reflect OTP scenario. |
| 10.07 or earlier | --                                       |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

### ip dns domain-list

```
ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
no ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
```

#### Description

Configures one or more domain names that are appended to the DNS request. The DNS client appends each name in succession until the DNS server replies. Domains can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF.

The **no** form of this command removes a domain from the list.

| Parameter                             | Description                                                                                       |
|---------------------------------------|---------------------------------------------------------------------------------------------------|
| <code>list &lt;DOMAIN-NAME&gt;</code> | Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters. |
| <code>vrf &lt;VRF-NAME&gt;</code>     | Specifies a VRF name. Default: default.                                                           |

#### Examples

This example defines a list with two entries: **domain1.com** and **domain2.com**.

```
switch(config)# ip dns domain-list domain1.com
switch(config)# ip dns domain-list domain2.com
```

This example defines a list with two entries, **domain2.com** and **domain5.com**, with requests being sent on **mainvrf**.

```
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain5.com vrf mainvrf
```

This example removes the entry **domain1.com**.

```
switch(config)# no ip dns domain-list domain1.com
```



For more information on features that use this command, refer to the Fundamentals Guide or the IP Services Guide for your switch model.

#### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip dns domain-name

```
ip dns domain-name <DOMAIN-NAME> [vrf <VRF-NAME>]
no ip dns domain-name <DOMAIN-NAME> [vrf <VRF-NAME>]
```

### Description

Configures a domain name that is appended to the DNS request. The domain can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF. If a domain list is defined with the command `ip dns domain-list`, the domain name defined with this command is ignored.

The **no** form of this command removes the domain name.

| Parameter                         | Description                                                                       |
|-----------------------------------|-----------------------------------------------------------------------------------|
| <code>&lt;DOMAIN-NAME&gt;</code>  | Specifies the domain name to append to DNS requests. Length: 1 to 256 characters. |
| <code>vrf &lt;VRF-NAME&gt;</code> | Specifies a VRF name. Default: default.                                           |

### Examples

Setting the default domain name to `domain.com`:

```
switch(config)# ip dns domain-name domain.com
```

Removing the default domain name `domain.com`:

```
switch(config)# no ip dns domain-name domain.com
```



For more information on features that use this command, refer to the Fundamentals Guide or the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip dns host

```
ip dns host <HOST-NAME> <IP-ADDR> [vrf <VRF-NAME>]
no ip dns host <HOST-NAME> <IP-ADDR> [vrf <VRF-NAME>]
```

### Description

Associates a static IP address with a hostname. The DNS client returns this IP address instead of querying a DNS server for an IP address for the hostname. Up to six hosts can be defined. If no VRF is defined, the default VRF is used.

The **no** form of this command removes a static IP address associated with a hostname.

| Parameter        | Description                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host <HOST-NAME> | Specifies the name of a host. Length: 1 to 256 characters.                                                                                                                                                                 |
| <IP-ADDR>        | Specifies an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. |
| vrf <VRF-NAME>   | Specifies a VRF name. Default: default.                                                                                                                                                                                    |

### Examples

This example defines an IPv4 address of **3.3.3.3** for **host1**.

```
switch(config)# ip dns host host1 3.3.3.3
```

This example defines an IPv6 address of **b::5** for **host 1**.

```
switch(config)# ip dns host host1 b::5
```

This example defines removes the entry for **host 1** with address **b::5**.

```
switch(config)# no ip dns host host1 b::5
```



For more information on features that use this command, refer to the Fundamentals Guide or the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip dns server address

```
ip dns server-address <IP-ADDR> [vrf <VRF-NAME>]
no ip dns server-address <IP-ADDR> [vrf <VRF-NAME>]
```

### Description

Configures the DNS name servers that the DNS client queries to resolve DNS queries. Up to six name servers can be defined. The DNS client queries the servers in the order that they are defined. If no VRF is defined, the default VRF is used.

The **no** form of this command removes a name server from the list.

| Parameter      | Description                                                                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP-ADDR>      | Specifies an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. |
| vrf <VRF-NAME> | Specifies a VRF name. Default: default.                                                                                                                                                                                    |

### Examples

This example defines a name server at **1.1.1.1**.

```
switch(config)# ip dns server-address 1.1.1.1
```

This example defines a name server at **a::1**.

```
switch(config)# ip dns server-address a::1
```

This example removes a name server at **a::1**.

```
switch(config)# no ip dns server-address a::1
```



For more information on features that use this command, refer to the Fundamentals Guide or the IP Services Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip dns fqdn-resolver refresh-interval

[no] ip dns fqdn-resolver refresh-interval <3600-86400>

### Description

Sets the refresh interval for FQDN resolvers. The interval specifies the time in seconds after which the FQDN resolver entries are refreshed. The valid range for the interval is between 3600 seconds (1 hour) to 86400 seconds (1 day). For each FQDN entry refresh timer is applicable from the time entry is installed.

The **no** form of this command removes the refresh interval and sets it back to default value which is 1 day.

| Parameter    | Description                                                              |
|--------------|--------------------------------------------------------------------------|
| <3600-86400> | Refresh interval in seconds (default: 86400 seconds).<br><i>Required</i> |

### Examples

This example sets a custom refresh interval.

```
switch(config)# ip dns fqdn-resolver refresh-interval 6000
switch(config)# ip dns fqdn-resolver refresh-interval 85400
```

Resetting the refresh interval to the default value.

```
switch(config)# no ip dns fqdn-resolver refresh-interval
```

Attempting to set an invalid interval:

```
switch(config)# ip dns fqdn-resolver refresh-interval 20
Invalid interval. Valid range: 3600-86400 seconds.
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip dns fqdn-resolver force-refresh

```
ip dns fqdn-resolver force-refresh { fqdn WORD | source port-access | vrf WORD | status
(resolved | stale | unresolved) }
```

### Description

This command initiates a force refresh for FQDN resolver entry/entries. It can refresh all FQDN entries, or entries filtered by FQDN, source, VRF or status. If no FQDN is specified, all entries are refreshed.

| Parameter | Description                                                                      |
|-----------|----------------------------------------------------------------------------------|
| fqdn      | Refresh entries associated with specific FQDN.<br><i>Optional</i>                |
| vrf       | Refresh entries associated with a specific VRF.<br><i>Optional</i>               |
| status    | Refresh entries associated with a specific resolution status.<br><i>Optional</i> |



The **source** parameter is not supported in 8320, 8400 or 9300 switch series.

### Examples

Refreshing all FQDN entries:

```
switch(config)# ip dns fqdn-resolver force-refresh
```

Refreshing a specific FQDN:

```
switch(config)# ip dns fqdn-resolver force-refresh fqdn www.example.com
```

Refreshing FQDN in a specific VRF:

```
switch(config)# ip dns fqdn-resolver force-refresh fqdn www.example.com vrf red
```

Refreshing FQDN for a specific source and vrf:

```
switch(config)# ip dns fqdn-resolver force-refresh source classifier vrf red
```

When a FQDN entry is not found:

```
switch(config)# ip dns fqdn-resolver force-refresh fqdn www.nonexistent.com
No FQDN entries matching the given criteria.
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show ip dns

```
show ip dns [vrf <VRF-NAME>] [vsx-peer]
```

### Description

Shows all DNS client configuration settings or the settings for a specific VRF.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf <VRF-NAME> | Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.                                                                                                                                  |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Usage

DNS client arbitration on the MGMT interface on a MGMT VRF can be updated via three different methods.

1. Using the **domain-name <name>** or **nameservers <servers>** commands in the command-line interface.
2. Using the **ip dns domain-name <DOMAIN-NAME> vrf MGMT** or **ip dns server-address <SERVER> vrf MGMT** commands in the command-line interface.
3. Using the **ip dhcp** command in the command-line interface (dynamic entries).

AOS-CX gives the following priority levels to the these three update methods.



- Priority 1 - standalone CLI configuration
- Priority 2 - static ip dns configuration
- Priority 3 - Dynamic config

## Examples

These examples define DNS settings and then show how they are displayed with the **show ip dns** command.

```
switch(config)# ip dns domain-name domain.com
switch(config)# ip dns domain-list domain5.com
switch(config)# ip dns domain-list domain8.com
switch(config)# ip dns server-address 4.4.4.4
switch(config)# ip dns server-address 6.6.6.6
switch(config)# ip dns host host3 5.5.5.5
switch(config)# ip dns host host2 2.2.2.2
switch(config)# ip dns host host3 c::12
switch(config)# ip dns domain-name reddomain.com vrf red
switch(config)# ip dns domain-list reddomain5.com vrf red
switch(config)# ip dns domain-list reddomain8.com vrf red
switch(config)# ip dns server-address 4.4.4.5 vrf red
switch(config)# ip dns server-address 6.6.6.7 vrf red
switch(config)# ip dns host host3 5.5.5.6 vrf red
switch(config)# ip dns host host2 2.2.2.3 vrf red
switch(config)# ip dns host host3 c::13 vrf red
switch# show ip dns
VRF Name : default
```

```
Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6
```

| Host Name | Address |
|-----------|---------|
| host2     | 2.2.2.2 |
| host3     | 5.5.5.5 |
| host3     | c::12   |

VRF Name : red

```
Domain Name : reddomain.com
DNS Domain list : reddomain5.com, reddomain8.com
Name Server(s) : 4.4.4.5, 6.6.6.7
```

| Host Name | Address |
|-----------|---------|
| host2     | 2.2.2.3 |
| host3     | 5.5.5.6 |
| host3     | c::13   |

```
switch(config)# ip dns domain-name domain.com vrf red
switch(config)# ip dns domain-list domain5.com vrf red
switch(config)# ip dns domain-list domain8.com vrf red
switch(config)# ip dns server-address 4.4.4.4 vrf red
switch(config)# ip dns server-address 6.6.6.6 vrf red
switch(config)# ip dns host host3 5.5.5.5 vrf red
switch(config)# no ip dns host host2 2.2.2.2 vrf red
switch(config)# ip dns host host3 c::12 vrf red
```

```

switch# show ip dns vrf red
VRF Name : red

Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6

Host Name Address

host3 5.5.5.5
host3 c::12

```



For more information on features that use this command, refer to the Fundamentals Guide or the IP Services Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ip dns fqdn-resolver

```
show ip dns fqdn-resolver
```

## Description

This command displays a summary table of all FQDN resolver entries, including the total count of FQDN entries, refresh time, source information, and a tabular display of all entries.

## Examples

Show unresolved FQDN entries with ipv4 requested:

```

switch# show ip dns fqdn-resolver
Total FQDN: 1
Refresh Time: 86400 seconds

Source: port-access
VRF FQDN Status Addr-Family ip-address

--
default host1.search.com unresolved ipv4 -

```

Show resolved FQDN entries:

```
switch# show ip dns fqdn-resolver
```

```
Total FQDN: 2
```

```
Refresh Time: 7200 seconds
```

```
Source: port-access
```

| VRF          | FQDN                  | Status   | Addr-Family | ip-address |
|--------------|-----------------------|----------|-------------|------------|
| default      | www.example.com       | resolved | ipv4        |            |
| 192.168.1.1, | 192.168.1.2           |          |             |            |
| default      | api.test.com          | resolved | ipv4        | 10.0.0.1   |
|              |                       |          | ipv6        |            |
| 2001:db8::1, | 2001:db8::2           |          |             |            |
| long_vrf_na  | a_very_long_fqdn_name | resolved | ipv4        | 10.0.0.2   |

When no FQDN entries exist:

```
switch(config)# show ip dns fqdn-resolver
```

```
No FQDN resolver entries found.
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show ip dns fqdn-resolver detail

```
show ip dns fqdn-resolver detail
```

```
{fqdn WORD | source port-access | vrf WORD | requested-address-family (ipv4 | ipv6 | both)}
```

## Description

Displays detailed hierarchical information for FQDN resolver entries, including the FQDN, VRF, requested address family, resolved IPv4 and IPv6 addresses, resolution status, and remaining refresh timer. The command supports filtering by FQDN, source, VRF, and address family. If no filters are provided, all entries are displayed.

## Examples

Show detailed view with unresolved entry:

```
switch# show ip dns fqdn-resolver detail

Source: port-access

FQDN: host1.search.com
VRF: default
Requested Address Family: ipv4
Status: unresolved

```

Show detailed view with resolved entries:

```
switch# show ip dns fqdn-resolver detail
Source: port-access
 FQDN: www.example.com
 VRF: default
 Status: resolved
 Requested Address Family: both
 IPv4 Addresses:
 192.168.1.1
 IPv6 Addresses:
 2001:db8::1
 2001:db8::2

 FQDN: www.hpe.com
 VRF: default
 Status: resolved
 Requested Address Family: ipv4
 IPv4 Addresses:
 10.0.0.1

```

Show detailed view with filter:

```
switch# show ip dns fqdn-resolver detail fqdn www.example.com
Source: port-access
 FQDN: www.example.com
 VRF: default
 Status: resolved
 Requested Address Family: both
 IPv4 Addresses:
 192.168.1.1
 192.168.1.2
 IPv6 Addresses:
 2001:db8::1
 2001:db8::2

```

Show detailed view when no entries exist:

```
switch# show ip dns fqdn-resolver detail
No FQDN resolver entries found
```



---

The **source** parameter is not supported in 8320, 8400 or 9300 switch series.

---



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show ip dns fqdn-resolver refresh-interval

```
show ip dns fqdn-resolver refresh-interval
```

## Description

Displays the current refresh interval for FQDN resolvers.

## Examples

Show current refresh interval (default):

```
switch# show ip dns fqdn-resolver refresh-interval
Refresh Interval: 86400 seconds
```

Show refresh interval after configuration change:

```
switch(config)# ip dns fqdn-resolver refresh-interval 7200
switch(config)# exit
switch# show ip dns fqdn-resolver refresh-interval
Refresh Interval: 7200 seconds
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

ip ecmp dynamic-mode

```
ip ecmp dynamic-mode {(flow-based [inactivity-timeout <256-16384>] | packet-based) outer-
header }
```

```
[no] ip ecmp dynamic-mode {(flow-based [inactivity-timeout <256-16384>] | packet-based)
outer-header }
```

Description

Specifies the ECMP dynamic mode and its parameters to be used while doing ECMP dynamic load balancing. The no form of this command disables dynamic mode load balancing.

Using the no form of DLB mode that is not currently configured, for example **no ip ecmp dynamic-mode flow-based outer-header** while packet based load balancing is enabled has no effect. Finally, the shortened **no ip ecmp dynamic-mode** command unconfigures `_either_` DLB mode, and if no DLB load balancing mode is configured the command has no effect.

| Parameter                               | Description                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------|
| <code>&lt;inactivity-timeout&gt;</code> | Specifies the inactivity-timeout duration range (Default: 256 microseconds) |
| <code>&lt;outer-header&gt;</code>       | Specifies the Dynamic load-balancing based on outer-header.                 |

Examples

Specifying flow-based dynamic mode with inactivity time of 512 microseconds and dynamic load-balancing based on outer-header:

```
switch(config)# ip ecmp dynamic-mode flow-based inactivity-timeout 512 outer-
header
Modifying ECMP load balancing may cause a brief period of packet loss and
disrupt the network.
Continue (y/n)?
```

Specifying flow-based dynamic mode with the default inactivity-timeout and dynamic load-balancing based on outer-header:

```
switch(config)# ip ecmp dynamic-mode flow-based outer-header
Modifying ECMP load balancing may cause a brief period of packet loss and
disrupt the network.
Continue (y/n)?
```

Specifying packet-based dynamic mode and dynamic load-balancing based on outer-header:

```
switch(config)# ip ecmp dynamic-mode packet-based outer-header
Modifying ECMP load balancing may cause a brief period of packet loss and
disrupt the network.
Continue (y/n)?
```

Removing flow-based dynamic mode:

```
switch(config)# no ip ecmp dynamic-mode flow-based outer-header
Modifying ECMP load balancing may cause a brief period of packet loss and
disrupt the network.
Continue (y/n)?
```

Removing packet-based dynamic mode:

```
switch(config)# no ip ecmp dynamic-mode packet-based outer-header
Modifying ECMP load balancing may cause a brief period of packet loss and
disrupt the network.
Continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release    | Modification       |
|------------|--------------------|
| 10.14.1000 | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## show ip ecmp

```
show ip ecmp [vsx-peer]
```

### Description

Displays the Equal Cost Multipath (ECMP) configuration.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples



Showing output for HPE Aruba Networking 9300, 9300S switch Series:  
Flow-based with the default inactivity-timeout:

```
switch# show ip ecmp

ECMP Configuration

ECMP Status : Enabled

Dynamic Load Balancing Mode

Mode : Flow-based
Inactivity-timeout : 256 us

ECMP Load Balancing by

Source IP : Enabled
Destination IP : Enabled
Source Port : Enabled
Destination Port : Enabled
```

Packet-based with the default inactivity-timeout:

```
switch# show ip ecmp

ECMP Configuration

ECMP Status : Enabled

Dynamic Load Balancing Mode

Mode : Packet-based

ECMP Load Balancing by

Source IP : Enabled
Destination IP : Enabled
Source Port : Enabled
Destination Port : Enabled
```

Dynamic load-balancing has been removed:

```
switch# show ip ecmp

ECMP Configuration

ECMP Status : Enabled

Dynamic Load Balancing Mode

```

```
Mode : None
```

```
ECMP Load Balancing by
```

```

```

```
Source IP : Enabled
```

```
Destination IP : Enabled
```

```
Source Port : Enabled
```

```
Destination Port : Enabled
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                                       |
|------------------|----------------------------------------------------|
| 10.14.1000       | Command supported on 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                 |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## clear erps ring <RINGID> instance <ID>

```
clear erps ring <RINGID> instance <ID>
```

### Description

Removes the protection switching and triggers reversion both in revertive and non-revertive operation. This command will not change the configured revertive operation mode.

| Parameter | Description                                                  |
|-----------|--------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239.        |
| <ID>      | Required, specifies the ID of the ring instance. Range: 1-2. |

### Examples

Removes the protection switching and triggers reversion for ring 3, instance 2:

```
switch# clear erps ring 3 instance 2
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## clear erps statistics

```
clear erps statistics [ring <ID>] [instance <ID>]
```

### Description

This command clears the ERPS statistics for a ring or a ring instance.

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| <RINGID>  | Optional, specifies the ID of the ring. Range: 1-239.         |
| <ID>      | Optional, specifies the ID of the ring instance. Range: 1-64. |

## Examples

Clear ERPS statistics for ring 1:

```
switch# clear erps statistics ring 1
```

Clear ERPS statistics for instance 1 of ring 1:

```
switch# clear erps statistics ring 1 instance 1
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## erps ring

```
erps ring <RINGID>
no erps ring <RINGID>
```

### Description

This command creates an ERPS ring with a given ID.

The **no** form of this command removes all the configurations of the ring, including instances.

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239 |

## Examples

Create an ERPS ring:

```
switch(config)# erps ring 2
switch(config-ring-2)#
```

Remove an ERPS ring:

```
switch(config)# no erps ring 2
switch(config-ring-2)#
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> <port0|port1> interface

```
erps ring <RINGID>
 <port0|port1> interface <ifname>
```

### Description

This command configures the ERPS ring member port. An L2 interface in the switch is associated to one of the two member ports of an ERPS ring. In case of an interconnection node, only port0 is applicable for the sub-ring.

The **no** form of this command removes the association of the ring port to the L2 interface on the switch.

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239 |
| <PORT0>   | Required, set port0 of the ring.                     |
| <PORT1>   | Required, set port1 of the ring.                     |
| <ifname>  | Required, interface name (string).                   |

### Examples

Configure the ERPS ring member port:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# port0 interface 1/1/1
```

Remove the association of the ring port to the L2 interface on the switch:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no port0
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> description

```
erps ring <RINGID>
 description <LINE>
```

### Description

This command adds descriptive information to help administrators and operators understand the purpose of a ring. 1-64 printable ASCII characters are allowed.

The **no** form of this command removes the ring instance description.

| Parameter | Description                                                                |
|-----------|----------------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239                       |
| <LINE>    | Required, specifies the description text. Maximum length is 64 characters. |

### Examples

Add descriptive information to a ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3) description HPE RnD ring
```

Remove descriptive information from a ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3) no description
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring-<ringid> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> guard-interval

```
erps ring <RINGID>
 guard-interval <10 milliseconds>
```

### Description

Guard timer is used in nodes recovering from a local failure to avoid loops due to earlier Signal Fail (SF) messages that may be in the ring.

The configuration specifies the guard timer duration in units of 10 ms. The timer period must be greater than the maximum expected forwarding delay in which an R-APS message traverses the entire ring. The default value is 50.

The **no** form of this command removes the configured value of the guard interval and sets it to the default value of 50.

| Parameter         | Description                                                                  |
|-------------------|------------------------------------------------------------------------------|
| <RINGID>          | Required, specifies the ID of the ring. Range: 1-239                         |
| <10 milliseconds> | Required, specifies the guard timer duration in units of 10 ms. Default: 50. |

### Examples

Specify the guard timer duration:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# guard-interval 100
```

Remove the configured value of the guard interval and set it to the default value of 50:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no guard-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> hold-off-interval

```
erps ring <RINGID>
 hold-off-interval <100 milliseconds>
```

### Description

Specifies hold-off interval in units of 100 ms. If specified, a defect is not reported immediately. Instead, the hold-off timer is started. On expiration of the timer, if the defect still exists, it is reported to protection switching. The default value for hold-off timer is 0.

The **no** form of this command removes the configured value of the hold-off interval and sets it to the default value of 0.

| Parameter          | Description                                                               |
|--------------------|---------------------------------------------------------------------------|
| <RINGID>           | Required, specifies the ID of the ring. Range: 1-239                      |
| <100 milliseconds> | Required, specifies the hold-off interval in units of 100 ms. Default: 0. |

### Examples

Specify the hold-off interval:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# hold-off-interval 100
```

Remove the configured value of the hold-off interval and set it to the default value of 0:



```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no hold-off-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring-<ringid> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance

```
erps ring <RINGID>
 instance <ID>
```

### Description

On a common ERPS network, a physical ring can be configured with a single ERPS ring, and only one blocked port can be specified in the ring. When the ERPS ring is in normal state, the blocked port prohibits all service packets from passing through. As a result, all service data is transmitted through one path over the ERPS ring, and the other link on the blocked port becomes idle, leading to ineffective use of bandwidth.

To improve link use efficiency, logical rings can be configured in the same physical ring in the ERPS multi-instance. A port may have different roles in different ERPS rings and different ERPS rings use different control VLANs.

An ERPS ring must be configured with an ERP instance, and each ERP instance specifies a range of VLANs. The topology calculated for a specific ERPS ring only takes effect in the ERPS ring. Different VLANs can use separate paths, implementing traffic load balancing and link backup.

The **no** form of this command removes the instance of the ring.

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239               |
| <ID>      | Required, specifies the ERPS ring instance identifier. Range: 1-2. |

### Examples

Create a ring instance:

```
switch(config)# erps ring 3
switch(config-ring-3)# instance 2
```

Remove a ring instance:

```
switch(config)# erps ring 3
switch(config-ring-3)# no instance 2
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> control-vlan

```
erps ring <RINGID>
 instance <ID> control-vlan <VID>
```

### Description

This command adds a control-channel VLAN to a ring instance. In an ERPS ring, the control VLAN should be used only to forward RAPS PDUs and not service packets. All the devices in an ERPS ring instance must be configured with the same control VLAN, and different ERPS ring instances must use different control VLANs.

The **no** form of this command removes the control-channel VLAN of the ring instance.

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239               |
| <ID>      | Required, specifies the ERPS ring instance identifier. Range: 1-2. |
| <VID>     | Required, VLAN ID. Range: 1-4094.                                  |

### Examples

Add a control-channel VLAN to a ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) control-vlan 10
```

Remove the control-channel VLAN of the ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no control-vlan
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> description

```
erps ring <RINGID>
 instance <ID> description <LINE>
```

### Description

This command adds descriptive information to help administrators and operators understand the purpose of a ring instance. 1-64 printable ASCII characters are allowed.

The **no** form of this command removes the ring instance description.

### Command context

| Parameter | Description                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239                                                |
| <ID>      | Required, specifies the ERPS ring instance identifier. Range: 1-2.                                  |
| <LINE>    | Required, descriptive information about the ring instance. 1-64 printable ASCII characters allowed. |

### Examples

Add ring instance description:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) description HPE RnD DataVlan
```

Remove ring instance description:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no description
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> enable

```
erps ring <RINGID>
 instance <ID> enable
```

### Description

This configuration enables protection switching on the given instance of the ring. It is disabled by default.

The **no** form of this command disables protection switching on the given instance of the ring.

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239               |
| <ID>      | Required, specifies the ERPS ring instance identifier. Range: 1-2. |

### Examples

Enable protection switching on the given instance of the ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) enable
```

Disable protection switching on the given instance of the ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no enable
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> protected-vlans

```
erps ring <RINGID>
 instance <ID> protected-vlans <VID-LIST>
```

### Description

This command specifies the set of VLANs that are protected by this ring instance.

The **no** form of this command removes a set of VLANs that are protected by this ring instance.

| Parameter      | Description                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <RINGID>       | Required, specifies the ID of the ring. Range: 1-239                                                                                                             |
| <ID>           | Required, specifies the ERPS ring instance identifier. Range: 1-2.                                                                                               |
| <VLAN-ID-LIST> | Required, range of VLANs to be protected by this ring instance. Range: 1-4094.<br><br><b>NOTE:</b> The list of protected VLAN IDs can not exceed 254 characters. |

## Examples

Specify a set of VLANs that are protected by this ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) protected-vlans 1,10-50
```

Remove a set of VLANs that are protected by this ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no protected-vlans 11,13
```

The following example shows an command with invalid syntax because the <VLAN-ID-LIST> string exceeds 254 characters.

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2

switch(config-erps-ring-3-inst-2) protected-vlans 1,3,6,8-10,16,32,40,46,94,97-
100,103
108,112,120-121,128,136,144,160,176,192,199-200,208,224,228,232,236,240,300-
301,310
313,315,500-507,600-621,699,851,998,1001-1002,1004-1006,1008,1011,1018-1022,1027-
1029,1100
1102,1105-1121,1145,1147-1149,2500-2519, 2520
```

**Configured Protected VLAN string size cannot be more than 254 characters.**



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring-<ringid> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> protection-switch {manual|force} <PORT0>|<PORT1>

erps ring <RINGID> instance <ID> protection-switch [{manual|force} <PORT0>|<PORT1>]

## Description

Blocks a specific ring interface in one of the two following ways:

- **Force:** The switch blocks a specific ring interface regardless of the protection switching state of the ring instance.
- **Manual:** The switch blocks a specific ring interface if no other protection switch event is active on the ring instance.

The user can verify whether the protection-switch is successful by verifying the status of instance and port state over which this command is executed.



```
switch# erps ring 1 instance 1 protection-switch force port0
switch# show erps status
Status for ERPS Ring 1 Instance 1:
=====
Ring ID : 1
Instance ID : 1
Port0 : 1/1/5 (Block)
Port1 : 1/1/6 (Up)
Node Role (RPL) : Owner (port0)
Control VLAN : 50
Protected VLAN : 1-49
Subring (TCN) : No (No)
Revertive Operation : Revertive
MEG Level : 7
Transmission Interval : 5 sec
Guard Interval : 0 sec 500 ms
Hold-Off Interval : 0 sec 0 ms
WTR Interval : 1 min
Status : Forced-switch
Oper Down Reason : None
```

| Parameter     | Description                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <RINGID>      | Required, specifies the ID of the ring. Range: 1-239                                                                                                       |
| <ID>          | Required, specifies the ERPS ring instance identifier. Range: 1-2.                                                                                         |
| <i>manual</i> | A type of protection switch event in which the switch blocks a specific ring interface if no other protection switch event is active on the ring instance. |
| <i>force</i>  | A type of protection switch event in which the switch blocks a specific ring interface regardless of the protection switching state of the ring instance.  |

## Examples

Block ring 3, interface 2, port 0 if no other protection switch event is active on the ring instance:

```
switch# erps ring 3 instance 2 protection-switch manual port0
```

Block ring 3, instance 2, regardless of the protection switching state of the ring instance:

```
switch# erps ring 3 instance 2 protection-switch force port1
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## erps ring <RINGID> instance <ID> revertive

erps ring <RINGID> instance <ID> revertive

### Description

Configures the default revertive mode of operation for an ERPS ring. In revertive operation, after the conditions causing protection switching are cleared, traffic channels are restored to the recovered link blocking the RPL. This configuration is meaningful only on the RPL node.

The **no** form of this command configures non-revertive mode of operation for an ERPS ring. In non-revertive operation, the traffic channels continue to use the RPL, if it has not failed, after conditions causing protection switching are cleared. This configuration is meaningful only on the RPL node.

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239               |
| <ID>      | Required, specifies the ERPS ring instance identifier. Range: 1-2. |

### Examples

Configuring the default revertive mode of operation for ERPS ring 3, instance 2:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2)# revertive
```

Configuring non-revertive mode of operation for ERPS ring 3, instance 2:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2)# no revertive
```





For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> role

```
erps ring <RINGID>
 instance <ID> role <RPL-OWNER|RPL-NEIGHBOR>
```

### Description

In ERPS, there is a central node called RPL Owner Node which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbor Node. It uses R-APS control messages to coordinate the activities of switching on/off the RPL link.

This command specifies the role of the node as owner or neighbor.

The **no** form of this command removes the configuration of the node role from the instance.

| Parameter      | Description                                                                             |
|----------------|-----------------------------------------------------------------------------------------|
| <RINGID>       | Required, specifies the ID of the ring. Range: 1-239                                    |
| <ID>           | Required, specifies the ERPS ring instance identifier. Range: 1-2.                      |
| <RPL-OWNER>    | Blocks traffic at one end of the RPL. The blocked end sends out periodic R-APS.         |
| <RPL-NEIGHBOR> | Blocks traffic at one end of the RPL. The blocked end does not generate periodic R-APS. |

### Examples

Specify the role of the node as owner:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) role rpl-owner
```

Specify the role of the node as neighbor:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 3
switch(config-erps-ring-3-inst-2) role rpl-neighbour
```

Remove the configuration of the node role from the instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no role
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> instance <ID> rpl

```
erps ring <RINGID>
 instance <ID> rpl <port0|port1>
```

## Description

In ERPS, there is a central node called RPL Owner Node which blocks one of the ports to ensure that there is no loop formed for the Ethernet traffic. The link blocked by the RPL owner node is called the Ring Protection Link or RPL. The node at the other end of the RPL is known as RPL Neighbor Node. It uses R-APS control messages to coordinate the activities of switching the RPL link on and off.

This command specifies which of the ERPS ring ports is the RPL.

The **no** form of this command removes the RPL port configuration from the ERPS ring instance.

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239                 |
| <ID>      | Required, specifies the ERPS ring instance identifier. Range: 1-2.   |
| <PORT0>   | Required, configure port0 to be RPL port in this ERPS ring instance. |
| <PORT1>   | Required, configure port1 to be RPL port in this ERPS ring instance. |

## Examples

Configure port0 to be RPL port in this ERPS ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) role rpl-owner
switch(config-erps-ring-3-inst-2) rpl port0
```

Configure port1 to be RPL port in this ERPS ring instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 3
switch(config-erps-ring-3-inst-2) role rpl-neighbour
switch(config-erps-ring-3-inst-2) rpl port1
```

Remove the RPL port configuration from the ERPS ring Instance:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# instance 2
switch(config-erps-ring-3-inst-2) no rpl port0
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring-<ringid> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> meg-level

```
erps ring <RINGID>
 meg-level <-0-7>
```

### Description

The R-APS messages transmitted by ERPS take the form of OAM PDUs as defined in G.8013. Each OAM PDU is transmitted at a specified level known as the Maintenance Entity Group (MEG) level. This command configures the level with which the ERPS packets must be transmitted.

The **no** form of this command removes the configured MEG level and sets it to the default value of 7.

| Parameter | Description                                                |
|-----------|------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239       |
| <0-7>     | Required, specifies the meg-level. Range: 0-7. Default: 7. |

## Examples

Specify the meg-level:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# meg-level 4
```

Remove the configured meg-level and set it to the default value of 7:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no meg-level
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context           | Authority                                                                          |
|---------------|---------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring-<ringid> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> parent-ring

```
erps ring <RINGID>
 parent-ring <RINGID>
```

## Description

This command associates a sub-ring to a parent-ring and is required for the sub-ring to notify the parent-ring on change in topology.

The **no** form of this command removes the parent ring identifier.

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239        |
| <RINGID>  | Required, specifies the ID of the parent-ring. Range: 1-239 |

## Examples

Associate a sub-ring to a parent-ring:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# parent-ring 2
```

Remove a parent-ring identifier:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no parent-ring 2
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> sub-ring

```
erps ring <RINGID>
 sub-ring
```

### Description

This command is to configure a sub-ring. If not specified, the ring is a major-ring.

The **no** form of this command removes the sub-ring configuration of the ring and configures it to be a major-ring.

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239 |

## Examples

Configure a sub-ring:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# sub-ring
```

Remove the sub-ring configuration from ring 2 and configure it to be a major-ring:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# no sub-ring
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> tcn-propagation

```
erps ring <RINGID>
 tcn-propagation
```

### Description

This command is to configure a sub-ring interconnection node to pass a topology change notification to the ring instance for the parent ring whenever the topology of the sub-ring changes. The parent ring instance performs a Forwarding Database (FDB) flush and sends a protocol message to ensure that other nodes on the parent ring also perform an FDB flush.

The **no** form of this command disables topology change notifications.

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239 |

<RINGID>

Required, specifies the ID of the ring. Range: 1-239

### Examples

Configure topology change notifications:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# tcn-propagation
```

Disable topology change notifications:

```
switch(config)# erps ring 2
switch(config-erps-ring-2)# no tcn-propagation
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

# erps ring <RINGID> transmission-interval

```
erps ring <RINGID>
 transmission-interval <SECONDS>
```

## Description

Specifies the R-APS periodic transmission interval in units of seconds. Default is 5 seconds.

The **no** form of this command removes the configured value of the transmission interval and sets it to the default value of 5 seconds.

| Parameter | Description                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239                                                |
| <SECONDS> | Required, specifies the R-APS periodic transmission interval in units of seconds. Range: 5 seconds. |

## Examples

Specify the R-APS periodic transmission interval as 10 seconds:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# transmission-interval 10
```

Remove the configured value of the transmission interval and set it to the default value of 5 seconds:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no transmission-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erps ring <RINGID> wtr-interval

```
erps ring <RINGID>
 wtr-interval <MINUTES>
```

### Description

The RPL owner node uses a delay timer before initiating an RPL block in case of both revertive mode of operation or before reverting to idle state after clearing operator commands (FS, MS).

The Wait to Restore (WTR) timer can be configured in 1-minute increments up to 12 minutes. The default value is 5 minutes. When recovering from an SF, the delay timer must be long enough to allow the recovering network to become stable. In the default revertive mode of operation, the WTR timer is used to prevent frequent operation of protection switching due to intermittent SF defects.

The **no** form of this command removes the configured value of the wtr-interval and sets it to the default value of 5 minutes.

| Parameter | Description                                                               |
|-----------|---------------------------------------------------------------------------|
| <RINGID>  | Required, specifies the ID of the ring. Range: 1-239                      |
| <MINUTES> | Required, specifies the wtr-interval in minutes. Range: 1-12. Default: 5. |

### Examples

Specify the wtr-interval:

```
switch(config)# erps ring 3
switch(config-erps-ring-3)# wtr-interval 7
```

Remove the configured value of the wtr-interval and set it to the default value of 5 minutes:



```
switch(config)# erps ring 3
switch(config-erps-ring-3)# no wtr-interval
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                         | Authority                                                                          |
|---------------|-----------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-erps-ring- <i>&lt;ringid&gt;</i> | Administrators or local user group members with execution rights for this command. |

## show erps statistics

```
show erps statistics [ring <RINGID>] [instance <ID> [<PORT0>|<PORT1>]]
```

### Description

This command displays ERPS statistics. The statistics can be displayed for the ring, the instance, or the instance ports.

| Parameter | Description                                                  |
|-----------|--------------------------------------------------------------|
| <RINGID>  | Optional, specifies the ID of the ring. Range: 1-239.        |
| <ID>      | Optional, specifies the ID of the ring instance. Range: 1-2. |
| <PORT0>   | Optional, specifies the ring member port 0.                  |
| <PORT1>   | Optional, specifies the ring member port 1.                  |

## Examples

```
switch# show erps statistics ring 1

Statistics for ERPS ring 1 instance 1:
=====
 Port0 Port1
 ---- ----
Local Failures 4 1

R-APS Port0 (Tx/Rx) Port1 (Tx/Rx)
----- -
NR 1/1 1/1
```

|        |      |      |
|--------|------|------|
| NR, RB | 0/1  | 0/1  |
| SF     | 1/0  | 1/0  |
| MS     | 0/0  | 0/10 |
| FS     | 30/0 | 0/0  |

Statistics for ERPS ring 1 instance 2:

```

=====
 Port0 Port1
 ---- ----
Local Failures 4 1
R-APS Port0 (Tx/Rx) Port1 (Tx/Rx)

NR 1/1 1/1
NR, RB 0/1 0/1
SF 1/0 1/0
MS 0/0 0/10
FS 30/0 0/0

```

```

switch# show erps statistics
Statistics for ERPS Ring 1 Instance 1 :
=====
 Port0 Port1
 ---- ----
Local Failures 4 1
R-APS Port0 (Tx/Rx) Port1 (Tx/Rx)

NR 33/9 33/9
NR, RB 58/0 58/0
SF 4/0 4/0
MS 0/0 0/0
FS 0/0 0/0

```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show erps status

```
show erps status [ring <RINGID>] [instance <ID>]
```

## Description

This command displays detailed information about a specific ring or all instances of a ring. The ring instance may be in one of the following states:

- **Idle:** The ring instance is operational.
- **Initializing:** The ring instance is not operational.
- **Protection:** Protection switching has been triggered by a local or remote link failure.
- **Pending:** Pending clearance of a previous protection switch.
- **Down:** Ring instance is not active.
- **Manual-switch:** Manual protection switching triggered by Admin-down.
- **Force-switch:** Forced protection switching triggered by admin.

A ring instance has the following reasons for "down" state:

- **Disabled:** Ring instance is administratively disabled.
- **Inconsistent Port Config:** The same port is configured as port0 and port1 or RPL port is configured by Admin-down.
- **Incomplete Port Config:** Only one or no ring port is configured.
- **Protected VLANs Not Configured:** Protected VLAN list is empty.
- **Control VLAN Not Configured:** Control VLAN is not configured.

The ring ports can be in one of the following states:

- **Up:** Port forwards control and data traffic.
- **Blocked:** Port blocks both control and data traffic.

| Parameter | Description                                                  |
|-----------|--------------------------------------------------------------|
| <RINGID>  | Optional, specifies the ID of the ring. Range: 1-239.        |
| <ID>      | Optional, specifies the ID of the ring instance. Range: 1-2. |

## Examples

Show ERPS status for ring 1 and instance 1:

```
Status for ERPS Ring 1 Instance 1
=====
Ring ID : 1
Ring description : ring_1
Instance ID : 1
Instance description : inst_1
Port0 : 1/0/1 (Blocked)
Port1 : 1/0/2 (Up)
Node Role (RPL) : Owner (Port0)
Control VLAN : 100
Protected VLAN : None
Subring (TCN) : Yes (Yes)
Revertive Operation : Revertive
MEG Level : 1
Transmission Interval : 5 sec
Guard Interval : 500 ms
Hold-Off Interval : 1 sec
WTR Interval : 5 min
```

|                  |                                  |
|------------------|----------------------------------|
| Status           | : Initializing                   |
| Oper Down Reason | : Protected Vlans Not Configured |

Show ERPS status for ring 1:

```
switch# show erps status ring 1

Status for ERPS Ring 1 Instance 1
=====
Ring ID : 1
Ring description : ring_1
Instance ID : 1
Instance description : inst_1
Port0 : 1/0/1 (Blocked)
Port1 : 1/0/2 (Up)
Node Role (RPL) : Owner (Port0)
Control VLAN : 100
Protected VLAN : 1-10
Subring (TCN) : Yes (Yes)
Revertive Operation : Non-Revertive
MEG Level : 1
Transmission Interval : 5 sec
Guard Interval : 500 ms
Hold-Off Interval : 1 sec
WTR Interval : 5 min
Status : Idle
Oper Down Reason : None

Status for ERPS Ring 1 Instance 2
=====
Ring ID : 1
Ring description : ring_1
Instance ID : 2
Instance description : inst_2
Port0 : 1/0/3 (Blocked)
Port1 : 1/0/4 (Up)
Node Role (RPL) : Owner (Port0)
Control VLAN : 110
Protected VLAN : 20-30
Subring (TCN) : No
Revertive Operation : Revertive
MEG Level : 1
Transmission Interval : 5 sec
Guard Interval : 500 ms
Hold-Off Interval : 1 sec
WTR Interval : 5 min
Status : Admin-Down
Oper Down Reason : None
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show erps summary

show erps summary

### Description

This command displays a summary of the ERPS configuration and state for the ERPS ring instances.

### Examples

```
switch# show erps summary

ERPS Summary
=====

Flags: R - RPL, M - Major Ring, S - Sub Ring, T - TCN Enabled
 * - RPL port

Per-Instance Summary
=====
Ring Instance Port0 Port1 Status Flags
---- -
1 1 1/1/1 *1/1/2 Pending R,M
1 2 1/1/1 1/1/2 Idle M
2 1 *1/1/3 - Protection R,S,T
2 2 1/1/3 - Admin-down S,T
3 1 1/1/4 1/1/5 Manual-switch M
3 2 1/1/4 1/1/5 Force-switch M
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

### active-gateway

```
active-gateway {ip | ipv6} [<IP-ADDRESS>] [mac <MAC-ADDRESS>]
no active-gateway {ip | ipv6} [<IP-ADDRESS>] [mac]
```

#### Description

Configures an EVPN Anycast gateway that can be used on multiple VTEPs. The Active Gateway supports both IPv4 and IPv6 addresses. The Active Gateway MAC address used along with an IPv4 and IPv6 address must match on a given interface, for the EVPN Anycast Gateway solution to work as expected. Active Gateway and SVI sharing the same IP is supported for both IPv4 and IPv6 addresses. The Active Gateway IP for IPv6 should be a Link-Local IPv6 address if the default Gateway is learned via RA messages.

The **no** form of this command removes the active gateway for active-active routing.

| Parameter     | Description                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| ip            | Specifies the configuration of an IPv4 address.                                                                                                    |
| ipv6          | Specifies the configuration of an IPv6 address.                                                                                                    |
| <IP-ADDRESS>  | Specifies the IPv4 or IPv6 address. <ul style="list-style-type: none"><li>■ Syntax for IPv4: A.B.C.D</li><li>■ Syntax for IPv6: A:B::C:D</li></ul> |
| <MAC-ADDRESS> | Specifies the Virtual MAC address. Syntax: xx:xx:xx:xx:xx:xx                                                                                       |

#### Usage

Before configuring active gateway, confirm that an IP address is on the SVI that is in the same subnet as the active gateway IP you are trying to configure. If an active gateway IP does not have an SVI IP with the same subnet, the CLI allows the configuration, but the active gateway IP will not be programmed in the kernel, resulting the active gateway to be unreachable.

Active forwarding cannot be configured when ICMP redirect is enabled. Enter the **no ip icmp redirect** command for disabling ICMP redirect.

It is highly recommended that you use an IPv6 link-local address as a gateway (VIP) on the active gateway IPv6 configuration.

If VRRP or active forwarding is configured on an SVI, active gateway cannot be configured. Active gateway with overlapping networks is not allowed. Maximum of 16 unique virtual MACs are supported in a system.

The maximum number of supported active gateways per switch is 4,000. Since a maximum of 31 secondary IPv4 addresses can be configured on an SVI, 32 IPv4 active gateways (along with the primary

IPv4 address) can be configured per SVI with IP multinetting support. This support is also the same for IPv6 addresses.



---

Do not use peer system MAC address as an active-gateway VMAC. If same MAC address is used, the VSX synchronization will try to sync the configuration on secondary switch and cause traffic disruptions.

---

## Examples

Configuring active-gateway, showing the IP address is the same as the SVI IP address on both VSX peers (valid for IPv4 and IPv6):

Switch 1:

```
switch1(config-if-vlan) # ip address 192.168.1.250/24
switch1(config-if-vlan) # active-gateway ip 192.168.1.250 mac 00:00:00:00:00:01
switch1(config-if-vlan) # active-gateway ipv6 fe80::100 mac 00:00:00:00:00:01
switch1(config-if-vlan) # ipv6 address link-local fe80::100/64
```

Switch 2:

```
switch2(config-if-vlan) # ip address 192.168.1.250/24
switch2(config-if-vlan) # active-gateway ip 192.168.1.250 mac 00:00:00:00:00:01
switch2(config-if-vlan) # active-gateway ipv6 fe80::100 mac 00:00:00:00:00:01
switch2(config-if-vlan) # ipv6 address link-local fe80::100/64
```

Configuring only the active gateway address:

```
switch(config-if-vlan) # ip address 192.168.1.250/24
switch(config-if-vlan) # active-gateway ip 192.168.1.250
```

Configuring only the active gateway IP MAC address:

```
switch2(config-if-vlan) # ip address 192.168.1.250/24
switch2(config-if-vlan) # active-gateway ip mac 00:00:00:01:00:01
```

Removing the active gateway for active-active routing (IPv6 and IPv4):

```
switch(config-if-vlan) # no active-gateway ip
switch(config-if-vlan) # no active-gateway ipv6
```

Removing the active gateway for active-active routing for an IP address:

```
switch(config-if-vlan) # no active-gateway ip 192.168.1.250
```

Removing the active gateway for active-active routing for virtual MAC addresses:

```
switch(config-if-vlan) # no active-gateway ip mac
```

When configuring the virtual active gateway for IPv6 on an SVI, it is recommended to use the same global IPv6 and active gateway IPv6 address. Similarly, if you want to use the IPv6 link-local address for

the virtual active gateway then the same address should be configured for both the SVI and the active gateway.

Global IPv6 address:

```
switch(config-if-vlan)# ipv6 address 1001::1/64
switch(config-if-vlan)# active-gateway ipv6 1001::1
switch(config-if-vlan)# active-gateway ipv6 mac 00:00:00:00:aa:01
```

IPv6-Link-Local address:

```
switch(config-if-vlan)# ipv6 address link-local fe80::1/64
switch(config-if-vlan)# active-gateway ipv6 fe80::1
switch(config-if-vlan)# active-gateway ipv6 mac 00:00:00:00:aa:01
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification                                                                             |
|------------------|------------------------------------------------------------------------------------------|
| 10.09.0010       | Added IPv6 support for configuration of active gateway and SVI with the same IP address. |
| 10.07 or earlier | --                                                                                       |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Administrators or local user group members with execution rights for this command. |

## arp-suppression

```
arp-suppression
no arp-suppression
```

### Description

Enables ARP suppression for EVPN-VxLAN globally. When enabled, switch will respond to the broadcast or unicast ARP request if target address is present in the NDMD cache. Suppression is only supported for ARP packets received on access ports. Suppression is not supported for ARP packets received on tunnel (VxLAN). Disabled by default. **Show running-config all** will show the default ARP suppression values.

The **no** form of this command disables the ARP suppression.



One the 8325 and 10000 Switch Series arp-suppression cannot be enabled with **arp-suppression-extended**.

## Examples

Configuring ARP suppression in EVPN:



```
switch(config-evpn) # arp-suppression
switch(config-evpn) # no arp-suppression
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                 | Authority                                                                          |
|---------------|---------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn<br>config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

## arp-suppression {enable | disable}

```
arp-suppression {enable | disable}
no arp-suppression {enable | disable}
```

### Description

Enables ARP suppression for EVPN-VXLAN on a specific VLAN. By default, ARP suppression for individual VLANs is not enabled. Users must manually configure it to either enable or disable this feature.

The **no** form of this command reverts the VLAN to its default state, where ARP suppression is not active.

| Parameter                    | Description                            |
|------------------------------|----------------------------------------|
| <code>&lt;enable&gt;</code>  | Enable ARP suppression for this VLAN.  |
| <code>&lt;disable&gt;</code> | Disable ARP suppression for this VLAN. |

### Usage

Suppression is only supported for ARP packets received on access ports. ARP suppression for individual VLANs is supported for Active Gateway SVI IP addresses.

Suppression is not supported for ARP packets received on tunnel (VXLAN). ARP suppression-extended feature is not available for individual VLANs.

#### 1. Enabled globally, disabled at VLAN level:

If ARP suppression is enabled globally but explicitly disabled for a specific VLAN, the VLAN-specific configuration takes precedence over the global setting. As a result, ARP suppression will not operate for the VLAN where it has been explicitly disabled, even if it is enabled at the global level.

#### 2. Disabled globally, enabled at VLAN level:

If ARP suppression is disabled globally but explicitly enabled for a specific VLAN, the VLAN-level configuration overrides the global setting. ARP suppression will be active only for the VLANs where it is

explicitly enabled, regardless of the global configuration. All other VLANs will adhere to the global configuration and have ARP suppression disabled.

## Examples

Enabling ARP suppression on VLAN 10:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# arp-suppression enable
switch(config-evpn-vlan-10)#
switch(config-evpn-vlan-10)# end
switch# show running-config evpn
evpn
 vlan 10
 arp-suppression enable
 vlan 20
 arp-suppression disable
```

Removing ARP suppression on VLAN 10:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# no arp-suppression enable
switch(config-evpn-vlan-10)# end
```

ARP suppression on VLAN 20:

```
switch(config-evpn-vlan-20)# no arp-suppression disable
switch(config-evpn-vlan-20)# end
switch# show running-config evpn
evpn
 vlan 10
 vlan 20
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context                 | Authority                                                                          |
|---------------|---------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn<br>config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

## arp-suppression {enable | disable}

```
arp-suppression {enable | disable}
no arp-suppression {enable | disable}
```

## Description

Enables ARP suppression for EVPN-VXLAN on a specific VLAN. By default, ARP suppression for individual VLANs is not enabled. Users must manually configure it to either enable or disable this feature.

The **no** form of this command reverts the VLAN to its default state, where ARP suppression is not active.

| Parameter                    | Description                            |
|------------------------------|----------------------------------------|
| <code>&lt;enable&gt;</code>  | Enable ARP suppression for this VLAN.  |
| <code>&lt;disable&gt;</code> | Disable ARP suppression for this VLAN. |

## Usage

Suppression is only supported for ARP packets received on access ports. ARP suppression for individual VLANs is supported for Active Gateway SVI IP addresses.

Suppression is not supported for ARP packets received on tunnel (VXLAN). ARP suppression-extended feature is not available for individual VLANs.

### 1. Enabled globally, disabled at VLAN level:

If ARP suppression is enabled globally but explicitly disabled for a specific VLAN, the VLAN-specific configuration takes precedence over the global setting. As a result, ARP suppression will not operate for the VLAN where it has been explicitly disabled, even if it is enabled at the global level.

### 2. Disabled globally, enabled at VLAN level:

If ARP suppression is disabled globally but explicitly enabled for a specific VLAN, the VLAN-level configuration overrides the global setting. ARP suppression will be active only for the VLANs where it is explicitly enabled, regardless of the global configuration. All other VLANs will adhere to the global configuration and have ARP suppression disabled.

## Examples

Enabling ARP suppression on VLAN 10:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# arp-suppression enable
switch(config-evpn-vlan-10)#
switch(config-evpn-vlan-10)# end
switch# show running-config evpn
evpn
 vlan 10
 arp-suppression enable
 vlan 20
 arp-suppression disable
```

Removing ARP suppression on VLAN 10:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# no arp-suppression enable
switch(config-evpn-vlan-10)# end
```

ARP suppression on VLAN 20:

```

switch(config-evpn-vlan-20)# no arp-suppression disable
switch(config-evpn-vlan-20)# end
switch# show running-config evpn
evpn
 vlan 10
 vlan 20

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms | Command context  | Authority                                                                          |
|-----------|------------------|------------------------------------------------------------------------------------|
| 9300      | config-evpn      | Administrators or local user group members with execution rights for this command. |
| 9300S     | config-evpn-vlan |                                                                                    |

# arp-suppression exclude

[no] arp-suppression exclude <ip-address>

## Description

This command exempts certain IP addresses from ARP suppression and allows ARP requests for those IP addresses to be flooded across the VXLAN fabric even though the target addresses are present in the NDMD cache. For certain IP addresses, it may be necessary to allow ARP requests to be forwarded across the network even when suppression is enabled.

The **no** form of this command disables the IP exemption.



- ARP Suppression IP Exemption is not supported for arp-suppression-extended.
- Maximum IP addresses can be exempted from ARP Suppression per VLAN is 256.
- Maximum IP addresses can be exempted from ARP Suppression across all VLANs is 256.

## Examples

Configuring IP 10.1.1.1 exemption on VLAN 10:

```

switch(config-evpn-vlan-10)# arp-suppression
exclude Exclude specific IP address from ARP suppression
switch(config-evpn-vlan-10)# arp-suppression exclude 10.1.1.1
switch(config-evpn-vlan-10)# end

switch# show running-config evpn
evpn vlan 10

```

```
arp-suppression exclude 10.1.1.1
```

Removing IP 10.1.1.1 exemption on VLAN 10:

```
switch(config-evpn-vlan-10)# no arp-suppression exclude 10.1.1.1
switch(config-evpn-vlan-10)# end

switch# show running-config evpn
evpn
 vlan 10
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms              | Command context                 | Authority                                                                          |
|------------------------|---------------------------------|------------------------------------------------------------------------------------|
| 9300-32D<br>9300-32C8D | config-evpn<br>config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

# dyn-vxlan-tunnel-bridging-mode

```
dyn-vxlan-tunnel-bridging-mode ibgp-ebgp
no dyn-vxlan-tunnel-bridging-mode ibgp-ebgp
```

## Description

Specifies the `dyn-vxlan-tunnel-bridging-mode` and provides the configurations to enable bridging between dynamic tunnels (BGP-EVPN-provisioned VXLAN tunnels). By default, split-horizon is enabled for all dynamic tunnels; therefore, bridging is disabled between them.

The default value is NULL.

The **no** form of this command disables bridging between dynamic tunnels.

## Usage

- Configuration of static tunnels is not recommended on VTEPs where iBGP-eBGP split horizon is disabled.
- iBGP and eBGP tunnels are part of different broadcast groups and bridging is permitted between them.
- Route Targets (RTs) have to be manually configured by the user.

## Examples

Enabling bridging between dynamic tunnels:

```
switch(config-evpn)#dyn-vxlan-tunnel-bridging-mode ibgp-ebgp
```

Disabling bridging between dynamic tunnels:

```
switch(config-evpn)# no dyn-vxlan-tunnel-bridging-mode ibgp-ebgp
```



For more information on features that use this command, refer to the VXLAN Guide and Multicast Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.09   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

## disable (evpn vlan-aware-bundles)

disable

### Description

Disables the VLAN aware bundle instance.

### Examples

Disabling the VLAN aware bundle instance bundle\_1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# disable
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## enable(evpn vlan-aware-bundles)

enable

### Description

Enables the VLAN aware bundle instance.

### Examples

Enabling the VLAN aware bundle instance bundle\_1.

```
switch(config-evpn) # vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1) # enable
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

### Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## evpn

evpn  
no evpn

### Description

Specifies the EVPN context which provides the configurations for VLAN-based EVPN service mode. The **no** form of this command removes this configuration.

### Examples

Configuring the EVPN context:

```
switch(config) # evpn
switch(config-evpn) #
```

Removing the EVPN configuration context:

```
switch(config-evpn)# no evpn
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

## igmp-mld-proxy

```
igmp-mld-proxy
no igmp-mld-proxy
```

### Description

Enables optimized Layer 2 multicast by using SMET routes (EVPN Route Type 6). When enabled alongside IGMP or MLD snooping, SMET routes are advertised instead of IGMP or MLD messages, enhancing multicast efficiency. Additionally, this command triggers an IMET route update for all VNIs with the multicast flags extended community, setting the IGMP and MLD proxy bits. IGMP-MLD proxy is disabled by default.

The **no** form of this command removes the configuration of IGMP-MLD Proxy using EVPN Route type 6.

### Usage

Enabling this command switches the Layer 2 multicast operating mode from CX's native mode (using IGMP/MLD messages) to standards-based SMET routes within the fabric. IGMP/MLD snooping must be configured on all participating VTEPs in the multicast network. This command also automatically starts the multicast Querier functionality on all VNI-mapped VLANs, using the SVI IP if configured, or the globally configured Querier IP (**ip igmp snooping querier-address**) if no SVI is present. Additionally, enabling this sets the multicast flag extended community in the IMET route, triggering a tunnel reconfiguration that may briefly impact traffic.



This feature does not support multihoming (using Route Type 7 and 8).

## Examples

Configuring IGMP-MLD Proxy using EVPN Route type 6.

```
switch(config-evpn)# igmp-mld-proxy
```



Removing the configuration of IGMP-MLD Proxy using EVPN Route type 6.

```
switch(config-evpn)# no igmp-mld-proxy
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

## igmp-mld-proxy forward-to-non-proxy

```
igmp-mld-proxy forward-to-non-proxy
no igmp-mld-proxy forward-to-non-proxy
```

### Description

Enables the switch to always forward multicast traffic to the set of VTEPs that do not support IGMP or MLD proxies (RFC 9251). This includes any VTEP that has advertised an Inclusive Multicast Ethernet Tag (IMET) route for the BD without a Multicast Flags Extended Community. By default, **igmp-mld-proxy forward-to-non-proxy** is disabled.

The **no** form of this command disables the configuration.

### Usage

In a fabric with a mix of VTEP's that support IGMP-MLD Proxy and those that do not, this command allows the switch to forward multicast traffic to legacy devices that lack IGMP-MLD Proxy support. Normally, with snooping enabled, VLAN traffic does not reach these legacy devices. Enabling this feature ensures that legacy devices receive the traffic needed to serve it's attached receivers.

Enabling this on a fabric with a large number of legacy devices causes proxy-capable devices to forward multicast traffic to all legacy VTEPs, potentially impacting performance.



This configuration should only be used when there are non-IGMP/MLD Proxy-capable devices in the network with attached receivers.

This command is effective only when used in conjunction with IGMP/MLD Proxy and IGMP/MLD snooping. By default, traffic is not forwarded to non-proxy-capable devices unless these settings are enabled.

### Examples

Enabling the switch to always forward multicast traffic to the set of VTEPs that do not support IGMP or MLD proxies.

```
switch(config-evpn)# igmp-ml-d-proxy forward-to-non-proxy
```

Removing the configuration of always forwarding multicast traffic to the set of VTEPs that do not support IGMP or MLD proxies.

```
switch(config-evpn)# no igmp-ml-d-proxy forward-to-non-proxy
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

## mac-move-detection count timer

```
mac-move-detection count <MAC-MOVE-COUNT> timer <MAC-MOVE-TIMER>
no mac-move-detection count <MAC-MOVE-COUNT> timer <MAC-MOVE-TIMER>
```

### Description

Configures EVPN MAC dampening for duplicate MAC and MAC-move count and timer across VTEPs.

The **no** form of this command resets the value of the count and timer to the default values of 5 and 180 seconds respectively.



EVPN MAC dampening is always enabled. Links to the VTEPs must be always up for EVPN MAC dampening to be activated.

| Parameter              | Description                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| count <MAC-MOVE-COUNT> | Specifies the number of MAC-moves for MAC dampening to take effect. Range: 2 to 10. Default: 5.                                |
| timer <MAC-MOVE-TIMER> | Specifies the MAC-move time limit in seconds for MAC dampening to take effect. Range: 1 to 1000 seconds. Default: 180 seconds. |

## Examples

Configuring EVPN MAC dampening:

```
switch(config-evpn)# mac-move-detection count 6 timer 199
```

The above command dampens a MAC if the MAC moves six times within 199 seconds.

```
switch(config-evpn)# mac-move-detection count 8
```

The above command dampens a MAC if the MAC moves eight times within 180 seconds.

```
switch(config-evpn)# mac-move-detection timer 255
```

The above command dampens a MAC if the MAC moves five times within 255 seconds.



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

# nd-suppression

```
nd-suppression
no nd-suppression
```

## Description

Enables IPv6 nd suppression globally for EVPN-VxLAN. When enabled, the switch will respond to the IPv6 multicast or unicast neighbor solicitation if target address is present in the NDMD cache. Suppression is only supported for NS packets received on access ports. Suppression is not supported for NS packets received on tunnel (VxLAN). Disabled by default. **Show running-config all** will show the default ND suppression values.

The **no** form of this command disables ND suppression.



One the 8325 and 10000 Switch Series **nd-suppression** cannot be enabled with **nd-suppression-extended**.

## Examples

Configuring ND suppression in EVPN:

```
switch(config-evpn)# nd-suppression
switch(config-evpn)# no nd-suppression
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

## nd-suppression (enable | disable)

```
nd-suppression {enable | disable}
no nd-suppression {enable | disable}
```

### Description

Enables ND suppression for EVPN-VxLAN on specific VLAN. When enabled, the switch will reply to IPv6 multicast or unicast neighbor solicitation messages if the target address is found in the NDMD cache. The no form of this command resets ND suppression to default for EVPN-VxLAN on specific VLAN.

| Parameter              | Description                           |
|------------------------|---------------------------------------|
| <i>&lt;enable&gt;</i>  | Enable ND suppression for this VLAN.  |
| <i>&lt;disable&gt;</i> | Disable ND suppression for this VLAN. |

### Usage

Suppression is only supported for NS packets received on access ports.

Suppression is not supported for ND packets received on tunnel (VxLAN).

Per-VLAN suppression is not enabled by default. Users must manually configure it to enable or disable the feature.

Per-VLAN ND suppression is mutually exclusive with ND suppression extended.

ND suppression on a per-VLAN basis is supported for Active Gateway SVI IP addresses. However, per-VLAN ND suppression extended is not supported.

#### 1. Enabled globally, disabled at VLAN level:

When ND suppression is enabled globally but explicitly disabled for a specific VLAN, the VLAN-specific configuration takes precedence over the global setting.

ND suppression will not operate for the VLAN where it is explicitly disabled, even if it is enabled globally. All other VLANs will adhere to the global configuration and have ND suppression enabled.

## 2. Disabled globally, enabled at VLAN level:

When ND suppression is disabled globally but explicitly enabled for a specific VLAN, the VLAN-level configuration takes precedence over the global setting.

ND suppression will be active only for VLANs where it is explicitly enabled, overriding the global configuration. All other VLANs will follow the global configuration and have ND suppression disabled.

## Examples

Enabling ND suppression on VLAN 10:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# nd-suppression enable
switch(config-evpn-vlan-10)#
switch(config-evpn-vlan-10)# end
switch# show running-config evpn
evpn
 vlan 10
 nd-suppression enable
 vlan 20
 nd-suppression disable
```

ND suppression on VLAN 10:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# no nd-suppression enable
switch(config-evpn-vlan-10)# end
```

ND suppression on VLAN 20:

```
switch(config-evpn-vlan-20)# no nd-suppression disable
switch(config-evpn-vlan-20)# end
switch# show running-config evpn
evpn
 vlan 10
 vlan 20
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context                 | Authority                                                                          |
|---------------|---------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn<br>config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

# nd-suppression exclude (per VLAN)

[no] nd-suppression exclude <ipv6-address>

## Description

This command exempts certain IPv6 addresses from ND suppression and allows neighbor solicitation (NS) for those IPv6 addresses to be flooded across the VXLAN fabric even though the target addresses are present in the NDMD cache. For certain IPv6 addresses, it may be necessary to allow NS to be forwarded across the network even when suppression is enabled.

The **no** form of this command disables the IP exemption.



- ND Suppression IPv6 Exemption is not supported for nd-suppression-extended.
- Maximum IPv6 addresses can be exempted from ND Suppression per VLAN is 256.
- Maximum IPv6 addresses can be exempted from ND Suppression across all VLANs is 256.

## Examples

Configuring IP 100::1 exemption on VLAN 10:

```
switch(config-evpn-vlan-10)# nd-suppression
 exclude Exclude specific IP address from ND suppression
switch(config-evpn-vlan-10)# nd-suppression exclude 100::1
switch(config-evpn-vlan-10)# end

switch# show running-config evpn
evpn
 vlan 10
 nd-suppression exclude 100::1
```

Removing IP 100::1 exemption on VLAN 10:

```
switch(config-evpn-vlan-10)# no arp-suppression exclude 100::1
switch(config-evpn-vlan-10)# end

switch# show running-config evpn
evpn
 vlan 10
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms              | Command context                 | Authority                                                                          |
|------------------------|---------------------------------|------------------------------------------------------------------------------------|
| 9300-32D<br>9300-32C8D | config-evpn<br>config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

## rd

```
rd {auto | <AS-NUMBER:ID> | <IP-ADDRESS:ID>}
no rd {auto | <AS-NUMBER:ID> | <IP-ADDRESS:ID>}
```

### Description

Specifies a unique number prepended to the advertised routes within the VLAN. It ensures support for overlapping IP addresses and MACs across different tenants. The default value is NULL. Route Distinguisher (RD) has to be manually configured by a user.

The **no** form of this command removes the currently configured value.

| Parameter       | Description                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto            | Specifies automatic route filtering.                                                                                                                                                                                            |
| <AS-NUMBER:ID>  | Specifies the AS number. It can be a 1-byte or 4-byte value. If the AS number is a 2-byte value, the administrative number is a 4-byte value and if the AS number is 4-byte value, the administrative number is a 2-byte value. |
| <IP-ADDRESS:ID> | Specifies the IP address. It is a 4-byte value and the ID is 2 bytes.                                                                                                                                                           |

### Examples

Configuring Route Distinguisher for EVPN VLAN:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# rd 6800:1
switch(config-evpn)# vlan 20
switch(config-evpn-vlan-20)# rd auto
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context  | Authority                                                                          |
|---------------|------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

# rd (evpn vlan-aware-bundles)

```
rd {<AS-NUMBER:NN> | <IP-ADDRESS:NN>}
no rd {<AS-NUMBER:NN> | <IP-ADDRESS:NN>}
```

## Description

Specifies a unique number prepended to the EVPN routes, advertised in the context of any VLAN configured under an EVPN VLAN aware bundle instance.

The **no** form of this command removes this configuration.

| Parameter       | Description                                                                                                                                                                                                                                |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <AS-NUMBER:NN>  | Specifies the AS number. The AS number can be a 2-byte or 4-byte value. If the AS number is a 2-byte value, the administrative number is a 4-byte value and if the AS number is 4-byte value, the administrative number is a 2-byte value. |
| <IP-ADDRESS:NN> | Specifies the IP address. The IP address is a 4-byte value and the ID is a 2-byte value.                                                                                                                                                   |

## Usage

This command ensures the support for overlapping IPs and MACs across different tenants. **rd** should be manually configured. **rd** should be unique across all VLAN-based (VLANs) and VLAN-aware (bundles) service instances.

## Examples

Configuring rd 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# rd 6800:1
```

Removing rd 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no rd 6800:1
```

Configuring rd 1.2.3.4:55.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# rd 1.2.3.4:55
```

Removing rd 1.2.3.4:55.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no rd 1.2.3.4:55
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History



| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## redistribute host-route

```
redistribute host-route
no redistribute host-route
```

### Description

Enables type-2 route advertisement to include the L3VNI, RT, and router MAC of the associated IP-VRF. It is applicable only in Symmetric routing where L3VNI is configured.

The **no** form of this command disables the redistribution of host routes.

| Parameter  | Description                              |
|------------|------------------------------------------|
| host-route | Specifies redistribution of host routes. |

### Examples

Configuring Redistribute host-route in EVPN:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# redistribute host-route
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context  | Authority                                                                          |
|---------------|------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

## redistribute host-route (evpn vlan-aware-bundles)

```
redistribute host-route
no redistribute host-route
```

## Description

Enables EVPN Route Type-2 advertisement to include L3VNI, Route Target, and Router MAC of the associated IP-VRF in the EVPN VLAN Aware Bundles.

The **no** form of this command removes this configuration.

## Usage

This is only applicable in cases of symmetric routing where L3VNI is configured.

## Examples

Enabling route advertisement in VLAN aware bundle bundle\_1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# redistribute host-route
```

Removing the route advertisement in VLAN aware bundle bundle\_1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no redistribute host-route
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## redistribute local-mac

```
redistribute local-mac
no redistribute local-mac
```

## Description

Enables Type-2 route advertisement for local MAC address of the SVI interfaces corresponding to the EVPN-enabled VLANs.

The **no** form of this command disables the Type-2 route advertisement.

## Examples

```
switch(config)# evpn
switch(config)# redistribute local-mac
switch(config)# vlan 20
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-evpn     | Administrators or local user group members with execution rights for this command. |

## redistribute local-svi

```
redistribute local-svi
no redistribute local-svi
```

### Description

Enables type-2 route advertisement for the local IP address and MAC address of the SVI interfaces corresponding to the EVPN-enabled VLANs.

The **no** form of this command disables type-2 route advertisement for the local IP address and MAC address of the SVI interfaces corresponding to the EVPN-enabled VLANs.

### Examples

Enabling type-2 route advertisement:

```
switch(config)# evpn
switch(config-evpn)# redistribute local-svi
```

Disabling type-2 route advertisement:

```
switch(config)# evpn
switch(config-evpn)# no redistribute local-svi
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn     | Administrators or local user group members with execution rights for this command. |

## route-target

```
route-target {import | export | both} {auto | <AS-NUMBER:ID> | <IP-ADDRESS:ID>}
no route-target {import | export | both} {auto | <AS-NUMBER:ID> | <IP-ADDRESS:ID>}
```

### Description

Controls the import and export of VPN routes only to the systems in the network for which routes are needed. The default value is NULL. Route Targets (RT) have to be manually configured by a user.

The **no** form of this command removes the currently configured value.

| Parameter       | Description                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| import          | Configures the route-target to import EVPN routes.                                                                                                                                                                              |
| export          | Configures the route-target to export EVPN routes.                                                                                                                                                                              |
| both            | Configures the route-target to import and export EVPN routes.                                                                                                                                                                   |
| auto            | Specifies automatic route filtering.                                                                                                                                                                                            |
| <AS-NUMBER:ID>  | Specifies the AS number. It can be a 1-byte or 4-byte value. If the AS number is a 2-byte value, the administrative number is a 4-byte value and if the AS number is 4-byte value, the administrative number is a 2-byte value. |
| <IP-ADDRESS:ID> | Specifies the IP address. It is a 4-byte value and the ID is 2 bytes.                                                                                                                                                           |

### Examples

Configuring Route Targets for EVPN VLAN:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# route-target import 6800:1
switch(config-evpn-vlan-10)# route-target export 6800:1
switch(config-evpn)# vlan 20
switch(config-evpn-vlan-20)# route-target both 6900:1
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context  | Authority                                                                          |
|---------------|------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

## route-target auto mode

```
route-target auto mode legacy
no route-target auto mode legacy
```

### Description

Configures format alternatives for auto-generation of route-targets. Mode legacy indicates that the route targets are auto-generated based on RFC4364 which is in ASN:VNI format. By default, route-targets are auto-generated based on RFC8365. Only 2-byte ASN value auto-generation is supported in this version of AOS-CX. For 4-byte ASN, value of 23456(AS\_TRANS) will be used in place of ASN followed by VNI.

The **no** form of this command removes the currently configured value.

| Parameter | Description                                                                             |
|-----------|-----------------------------------------------------------------------------------------|
| legacy    | Configures to auto-generate route-target in ASN:VNI format. This parameter is required. |

### Examples

Configuring alternative route-targets for EVPN VLAN:

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)# route-target auto mode legacy
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

### Command Information

| Platforms     | Command context  | Authority                                                                          |
|---------------|------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

## route-target {evpn}

```
route-target {import | export | both} {auto | <AS-NUMBER:ID> | <IP-ADDRESS:ID>} evpn
no route-target {import | export | both} {auto | <AS-NUMBER:ID> | <IP-ADDRESS:ID>} evpn
```

### Description

Configures the route target (RT) for EVPN VRF to control the import and export of VPN routes only to the systems in the network for which routes are needed. The default value is NULL. Route targets have to be manually configured by a user. Route-targets will be auto-generated in ASN:VNI format when 'auto' is configured. For 4-byte ASN, value of 23456(AS\_TRANS) will be used in place of ASN followed by VNI.

The **no** form of this command removes the RT in EVPN VRF.

| Parameter       | Description                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| import          | Imports the VRF routes that match the RT.                                                                                                                                                                                       |
| export          | Exports the RT in the VRF routes.                                                                                                                                                                                               |
| both            | Configures both import and export of routes for the VRF.                                                                                                                                                                        |
| auto            | Specifies automatic route filtering.                                                                                                                                                                                            |
| <AS-NUMBER:ID>  | Specifies the AS number. It can be a 1-byte or 4-byte value. If the AS number is a 2-byte value, the administrative number is a 4-byte value and if the AS number is 4-byte value, the administrative number is a 2-byte value. |
| <IP-ADDRESS:ID> | Specifies the IP address. It is a 4-byte value and the ID is 2 bytes.                                                                                                                                                           |

### Examples

Configuring Route Targets for EVPN VRF:

```
switch(config-vrf) # route-target import 6800:1 evpn
switch(config-vrf) # route-target export 6800:1 evpn
switch(config-vrf) # route-target both 6800:1 evpn
switch(config-vrf) # route-target import auto evpn
switch(config-vrf) # route-target export auto evpn
switch(config-vrf) # route-target both auto evpn
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vrf      | Administrators or local user group members with execution rights for this command. |

## route-target (evpn vlan-aware-bundles)

```
route-target {import | export | both} {<AS-NUMBER:ID> | <IP-ADDRESS:ID>}
no route-target {import | export | both} {<AS-NUMBER:ID> | <IP-ADDRESS:ID>}
```

### Description

Enables the import and export of EVPN routes only to the systems in the network for which routes are needed.

The **no** form of this command removes this configuration.

| Parameter       | Description                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| import          | Configures the route-target to import EVPN routes.                                                                                                                                                                              |
| export          | Configures the route-target to export EVPN routes.                                                                                                                                                                              |
| both            | Configures the route-target to import and export EVPN routes.                                                                                                                                                                   |
| <AS-NUMBER:ID>  | Specifies the AS number. It can be a 2-byte or 4-byte value. If the AS number is a 2-byte value, the administrative number is a 4-byte value and if the AS number is 4-byte value, the administrative number is a 2-byte value. |
| <IP-ADDRESS:ID> | Specifies the IP address. It is a 4-byte value and the ID is 2 bytes.                                                                                                                                                           |

### Usage

Route targets should be unique across all VLAN-based (VLANs) and VLAN-aware (bundles) service instances. `rt` should be manually configured.

### Examples

Configuring the import of route target 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# route-target import 6800:1
```

Removing the import of route target 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no route-target import 6800:1
```

Configuring the export of route target 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# route-target export 6800:1
```

Removing the export of route target 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no route-target export 6800:1
```

Configuring the import and export of route target 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# route-target both 6800:1
```

Removing the import and export of route target 6800:1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no route-target both 6800:1
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## show evpn evi

show evpn evi

### Description

Shows the information of EVPN instances.

### Examples

Showing information for EVPN instances:

```
switch# show evpn evi

L2VNI : 100
Route Distinguisher : 10.10.10.1:10
```



```

VLAN : 10
Status : Up
RT Import : 1.1.1.1:1, 2.2.2.2:1, 3.3.3.3:1, 5:1
RT Export : 4.4.4.4:61, 1000:21
Local MACs : 30
Remote MACs : 945
Peer VTEPs : 8

L2VNI : 200
Route Distinguisher :
VLAN : 20
Status : Down, No RD
RT Import : 1.1.1.1:2, 2.2.2.2:2, 3.3.3.3:2, 4.4.4.4:2,
 5.5.5.5:2, 5:2
RT Export : 4.4.4.4:62, 1000:22
Local MACs :
Remote MACs :
Peer VTEPs :

L2VNI : 300
Route Distinguisher : 10.10.10.1:30
VLAN : 30
Status : Up
RT Import : 1.1.1.1:3, 2.2.2.2:3, 3.3.3.3:3, 5:3
RT Export : 4.4.4.4:63, 1000:23
Local MACs : 30
Remote MACs : 945
Peer VTEPs : 12

L3VNI : 1000
Route Distinguisher : 10.10.10.1:1000
VRF : vrf1000
Status : Up
RT Import : 1.1.1.1:4, 2.2.2.2:4, 3.3.3.3:4, 5:4
RT Export : 4.4.4.4:64, 1000:24
Local Type-5 Routes : 2
Remote Type-5 Routes : 3
Peer VTEPs : 6

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn evi summary

show evpn evi summary

## Description

Shows the summary information for EVPN instances.

## Examples

Showing summary information for EVPN instances:

```
switch# show evpn evi summary

 L2VNI VLAN Status

 100 10 Up
 200 20 Down, RT conflict
 210 21 Up
 220 22 Down, No RT
 230 23 Down, No RT
 240 24 Up
 250 25 Up
 260 26 Up
 270 27 Up
 280 28 Up
 290 29 Up
 310 31 Up

 L3VNI VRF Status

 1000 vrf1000 Up
 1001 vrf1001 Down, RT conflict
 1002 vrf1002 Down, No RD
 1004 vrf1003 Down, Administratively down
 1005 vrf1003 Up

EVPN instances : 17
EVPN instances Up : 11
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn evi <EVI-ID>

```
show evpn evi <EVI-ID>
```

## Description

Shows the information for the particular EVPN instance.

| Parameter | Description                     |
|-----------|---------------------------------|
| <EVI-ID>  | Specifies the EVPN instance ID. |

## Examples

Showing information for the particular EVPN instance:

```
switch# show evpn evi 100
L2VNI : 100
 Route Distinguisher : 10.10.10.1:10
 VLAN : 10
 Status : Up
 RT Import : 1.1.1.1:1, 2.2.2.2:1, 3.3.3.3:1, 5:1
 RT Export : 4.4.4.4:61, 1000:21
 Local MACs : 30
 Remote MACs : 945
 Peer VTEPs : 8
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn evi detail

show evpn evi detail

### Description

Shows the detailed information for all EVPN instances.

### Examples

Showing detailed information for EVPN instances:

```
switch# show evpn evi detail

L2VNI : 100
 Route Distinguisher : 10.10.10.1:10
```

```

VLAN : 10
Status : Up
RT Import : 1.1.1.1:1, 2.2.2.2:1, 3.3.3.3:1, 5:1
RT Export : 4.4.4.4:61, 1000:21
Local MACs : 30
Remote MACs : 307
Peer VTEPs : 8

```

| Peer VTEPs | Remote MACs |
|------------|-------------|
| 10.10.10.2 | 40          |
| 10.10.10.3 | 22          |
| 10.10.10.4 | 15          |
| 10.10.10.5 | 155         |
| 10.10.10.6 | 25          |
| 10.10.10.7 | 35          |
| 10.10.10.8 | 50          |
| 10.10.10.9 | 55          |

#### L2VNI : 200

```

Route Distinguisher :
VLAN : 20
Status : Down, No RD
RT Import : 1.1.1.1:2, 2.2.2.2:2, 3.3.3.3:2, 4.4.4.4:2,
 5.5.5.5:2, 5:2
RT Export : 4.4.4.4:62, 1000:22
Local MACs :
Remote MACs :
Peer VTEPs :

```

| Peer VTEPs | Remote MACs |
|------------|-------------|
|------------|-------------|

#### L2VNI : 300

```

Route Distinguisher : 10.10.10.1:30
VLAN : 30
Status : Up
RT Import : 1.1.1.1:3, 2.2.2.2:3, 3.3.3.3:3, 5:3
RT Export : 4.4.4.4:63, 1000:23
Local MACs : 30
Remote MACs : 362
Peer VTEPs : 12

```

| Peer VTEPs  | Remote MACs |
|-------------|-------------|
| 10.10.10.2  | 60          |
| 10.10.10.3  | 12          |
| 10.10.10.4  | 13          |
| 10.10.10.5  | 15          |
| 10.10.10.6  | 15          |
| 10.10.10.7  | 35          |
| 10.10.10.8  | 53          |
| 10.10.10.9  | 45          |
| 10.10.10.10 | 11          |
| 10.10.10.11 | 12          |
| 10.10.10.12 | 35          |
| 10.10.10.13 | 56          |

#### L3VNI : 1000

```

Route Distinguisher : 10.10.10.1:1000
VRF : vrf1000
Status : Up

```

```

RT Import : 1.1.1.1:4, 2.2.2.2:4, 3.3.3.3:4, 5:4
RT Export : 4.4.4.4:64, 1000:24
Local Type-5 Routes : 2
Remote Type-5 Routes : 30
Peer VTEPs : 12

```

| Peer VTEPs  | Remote Type-5 Routes |
|-------------|----------------------|
| 10.10.10.2  | 2                    |
| 10.10.10.3  | 1                    |
| 10.10.10.4  | 1                    |
| 10.10.10.5  | 1                    |
| 10.10.10.6  | 1                    |
| 10.10.10.7  | 3                    |
| 10.10.10.8  | 5                    |
| 10.10.10.9  | 4                    |
| 10.10.10.10 | 1                    |
| 10.10.10.11 | 3                    |
| 10.10.10.12 | 3                    |
| 10.10.10.13 | 5                    |



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn evi <EVI-ID> detail

show evpn evi <EVI-ID> detail

### Description

Shows the detailed information for the particular EVPN instance.

| Parameter | Description                     |
|-----------|---------------------------------|
| <EVI-ID>  | Specifies the EVPN instance ID. |

### Examples

Showing detailed information for the particular EVPN instance:

```

switch# show evpn evi 100 detail
L2VNI : 100
 Route Distinguisher : 10.10.10.1:10
 VLAN : 10
 Status : Up
 RT Import : 1.1.1.1:1, 2.2.2.2:1, 3.3.3.3:1, 5:1
 RT Export : 4.4.4.4:61, 1000:21
 Local MACs : 30
 Remote MACs : 397
 Peer VTEPs : 8

 Peer VTEPs Remote MACs

 10.10.10.2 40
 10.10.10.3 22
 10.10.10.4 15
 10.10.10.5 155
 10.10.10.6 25
 10.10.10.7 35
 10.10.10.8 50
 10.10.10.9 55

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn evi igmp snooping

```
show evpn evi <EVI-ID> igmp snooping
```

### Description

Shows the information about the IGMP group memberships learned through EVPN. A default SMET route is identified by the Source and Group addresses set to 0.0.0.0 and is applicable for both IP versions.

| Parameter | Description                                        |
|-----------|----------------------------------------------------|
| <EVI-ID>  | Specifies the EVPN instance ID. Range: 1-16777214. |

### Examples

Showing information for a particular EVPN instance:

```
switch# show evpn evi igmp snooping
```

```
IGMP-MLD Proxy Status : Enabled
Forward to Non Proxy Status : Disabled
```

| EVI<br>Version | Source    | Group      | Next-hop         | Mode |   |
|----------------|-----------|------------|------------------|------|---|
| -----          |           |            |                  |      |   |
| 100            | 0.0.0.0   | 0.0.0.0    | vxlan1(11.1.1.4) | -    | - |
| 100            | 0.0.0.0   | 239.1.1.33 | vxlan1(11.1.1.3) | -    | 2 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.1) | INC  | 3 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.2) | INC  | 3 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.3) | INC  | 3 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.4) | INC  | 3 |
| 200            | 40.0.0.1  | 225.1.1.2  | vxlan1(11.1.1.3) | EXC  | 3 |
| 300            | 0.0.0.0   | 239.1.1.33 | vxlan1(11.1.1.5) | EXC  |   |
| 2,3            |           |            |                  |      |   |

Showing information for a particular EVPN instance:

```
switch# show evpn evi 200 igmp snooping
```

| EVI<br>Version | Source    | Group      | Next-hop         | Mode |   |
|----------------|-----------|------------|------------------|------|---|
| -----          |           |            |                  |      |   |
| 100            | 0.0.0.0   | 0.0.0.0    | vxlan1(11.1.1.4) | -    | - |
| 100            | 0.0.0.0   | 239.1.1.33 | vxlan1(11.1.1.3) | -    | 2 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.1) | INC  | 3 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.2) | INC  | 3 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.3) | INC  | 3 |
| 200            | 10.1.1.35 | 225.1.1.1  | vxlan1(11.1.1.4) | INC  | 3 |
| 200            | 40.0.0.1  | 225.1.1.2  | vxlan1(11.1.1.3) | EXC  | 3 |
| 300            | 0.0.0.0   | 239.1.1.33 | vxlan1(11.1.1.5) | EXC  |   |
| 2,3            |           |            |                  |      |   |



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn mac-ip

```
show evpn mac-ip
```

## Description

Show the information about the EVPN MAC-IP for the EVPN instances.

## Examples

Showing information about the EVPN MAC-IP for the EVPN instances:

```
switch# show evpn mac-ip
Flags: Local (L), Remote (R)
```

| EVI | MAC               | IP      | Next-hop          | Seq-Num | Flags |
|-----|-------------------|---------|-------------------|---------|-------|
| 100 | 14:50:56:96:76:56 |         | vxlan1 (11.1.1.3) | 0       | R     |
| 100 | 14:50:56:96:76:56 | 3.3.4.5 | vxlan1 (11.1.1.3) | 0       | R     |
| 100 | 14:50:56:96:76:56 | 3.3.5.5 | vxlan1 (11.1.1.3) | 0       | R     |
| 100 | 24:50:56:96:76:56 | 3.3.3.2 | vxlan1 (11.1.1.3) | 1       | R     |
| 100 | 34:50:56:96:76:56 | 3.3.6.2 |                   | 2       | L     |
| 100 | 44:50:56:96:76:56 | 3.3.7.3 |                   | 2       | L     |
| 200 | 52:50:56:96:76:56 | 5.5.5.2 |                   | 0       | L     |

```
MACs : 5
Remote MACs : 2
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn mac-ip evi

```
show evpn mac-ip evi <EVI-ID>
```

## Description

Show the information about the EVPN MAC-IP for the particular EVPN instance.

| Parameter | Description                     |
|-----------|---------------------------------|
| <EVI-ID>  | Specifies the EVPN instance ID. |

## Examples

Showing information about the EVPN MAC-IP for the particular EVPN instance:



```
switch# show evpn mac-ip evi 100
```

```
Flags: Local (L), Remote (R)
```

| MAC               | IP      | Next-hop          | Seq-Num | Flags |
|-------------------|---------|-------------------|---------|-------|
| 14:50:56:96:76:56 |         | vxlan1 (11.1.1.2) | 0       | R     |
| 14:50:56:96:76:56 | 3.3.4.5 | vxlan1 (11.1.1.3) | 0       | R     |
| 14:50:56:96:76:56 | 3.3.5.4 | vxlan1 (11.1.1.2) | 0       | R     |
| 24:50:56:96:76:56 | 3.3.3.2 | vxlan1 (11.1.1.3) | 1       | R     |
| 34:50:56:96:76:56 | 3.3.6.2 |                   | 2       | L     |
| 44:50:56:96:76:56 | 3.3.7.3 |                   | 2       | L     |

```
MACs : 4
```

```
Remote MACs : 2
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn evi mld snooping

```
show evpn evi <EVI-ID> mld snooping
```

### Description

Shows the information about the MLD group memberships learned through EVPN. A default SMET route is identified by the Source and Group addresses set to 0::0 and is applicable for both IP versions.

| Parameter | Description                                        |
|-----------|----------------------------------------------------|
| <EVI-ID>  | Specifies the EVPN instance ID. Range: 1-16777214. |

### Examples

Showing information for MLD group memberships learned through EVPN:

```
switch# show evpn evi mld snooping
```

| EVI      | Source | Group | Next-hop          | Mode |
|----------|--------|-------|-------------------|------|
| Version  |        |       |                   |      |
| -----100 | 0::0   | 0::0  | vxlan1 (11.1.1.4) | -    |

|     |         |          |                   |     |   |
|-----|---------|----------|-------------------|-----|---|
| 100 | 0::0    | ff12::c  | vxlan1 (11.1.1.4) | -   | 1 |
| 200 | 2000::1 | ff12::d  | vxlan1 (11.1.1.1) | INC | 2 |
| 200 | 2000::1 | ff12::d  | vxlan1 (11.1.1.2) | INC | 2 |
| 200 | 2000::1 | ff12::d  | vxlan1 (11.1.1.3) | INC | 2 |
| 200 | 2000::1 | ff12::d  | vxlan1 (11.1.1.4) | INC | 2 |
| 200 | 3000::1 | ff12::12 | vxlan1 (11.1.1.3) | EXC | 2 |
| 300 | 0::0    | ff12::c  | vxlan1 (11.1.1.5) | EXC |   |

1,2

Showing information for evi 200:

```
switch# show evpn evi 200 mld snooping
```

| EVI      | Source  | Group    | Next-hop          | Mode |   |
|----------|---------|----------|-------------------|------|---|
| Version  |         |          |                   |      |   |
| -----200 | 2000::1 | ff12::d  | vxlan1 (11.1.1.1) | INC  |   |
| 2        |         |          |                   |      |   |
| 200      | 2000::1 | ff12::d  | vxlan1 (11.1.1.2) | INC  | 2 |
| 200      | 2000::1 | ff12::d  | vxlan1 (11.1.1.3) | INC  | 2 |
| 200      | 2000::1 | ff12::d  | vxlan1 (11.1.1.4) | INC  | 2 |
| 200      | 3000::1 | ff12::12 | vxlan1 (11.1.1.3) | EXC  | 2 |



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show evpn vtep-neighbor

```
show evpn vtep-neighbor {all-vrfs | vrf <VRF-Name>}
```

### Description

Shows the remote VTEPs MAC-IP binding. The state of the peer VTEP denotes whether VXLAN tunnel to the VTEP is Up or Down.

| Parameter      | Description                                                                            |
|----------------|----------------------------------------------------------------------------------------|
| all-vrfs       | Display information for all VRFs.                                                      |
| vrf <vrf-name> | Specify a VRF by VRF name (if no <VRF-NAME> is specified, the default VRF is implied). |

## Examples

Showing EVPN VTEP neighbor information for all VRFs:

```
switch# show evpn vtep-neighbor all-vrfs
VTEP-IP L3VNI MAC VRF State

2.2.2.2 1234 00:20:56:bd:27:bc VRF1234 Up
2.2.2.2 6789 00:20:56:bd:27:bc VRF6789 Up
3.3.3.3 1234 00:30:56:ef:aa:cc VRF1234 Down
4.4.4.4 6789 00:40:56:12:34:44 VRF6789 Up
5.5.5.5 6789 00:50:56:ab:11:ee VRF6789 Up
```

Showing EVPN VTEP neighbor information for the specified VRF name:

```
switch# show evpn vtep-neighbor vrf VRF1234
VTEP-IP L3VNI MAC VRF State

2.2.2.2 1234 00:20:56:bd:27:bc VRF1234 Up
3.3.3.3 1234 00:30:56:ef:aa:cc VRF1234 Down
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show running-config evpn

```
show running-config evpn
```

### Description

Shows all EVPN configurations.

### Examples

Showing all EVPN configurations:

```
switch# show running-config evpn
evpn
 arp-suppression
 nd-suppression
```

```

vlan 10
 rd 2:2
 route-target both auto
vlan 20
 rd 3:3
 route-target both 3000:1
vlan-aware-bundle abcd10
 rd 10.10.10.10:10
 route-target export 200.200.200.200:200
 route-target import 100.100.100.100:100
 redistribute host-route
vlan 5-6
 vlan-ethernet-tag 5 20
 vlan-ethernet-tag 6 30

```

Showing EVPN configuration on the 8325 or 10000 Switch Series:

```

switch# show running-config evpn
evpn
 arp-suppression-extended
 nd-suppression-extended
 vlan 10
 rd 2:2
 route-target both auto
 vlan 20
 rd 3:3
 route-target both 3000:1
 vlan-aware-bundle abcd10
 rd 10.10.10.10:10
 route-target export 200.200.200.200:200
 route-target import 100.100.100.100:100
 redistribute host-route
 vlan 5-6
 vlan-ethernet-tag 5 20
 vlan-ethernet-tag 6 30

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification                                                                                                       |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| 10.16            | Updated example to include new <b>igmp-mld-proxy</b> and <b>igmp-mld-proxy forward-to-non-proxy</b> functionality. |
| 10.07 or earlier | --                                                                                                                 |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

# virtual-mac

```
virtual-mac <MAC-ADDR>
no virtual-mac <MAC-ADDR>
```

## Description

Configures the virtual MAC address for EVPN.

The **no** form of this command removes the virtual MAC address configuration.

| Parameter  | Description                        |
|------------|------------------------------------|
| <MAC-ADDR> | Specifies the virtual MAC address. |

## Examples

Configuring virtual MAC address for EVPN:

```
switch(config)# virtual-mac ab:12:33:33:03:22
```

Removing the configuration of the virtual MAC address for EVPN:

```
switch(config)# no virtual-mac ab:12:33:33:03:22
```



For EVPN symmetric IRB to work, `virtual-mac` must be configured and it must be unique for all the VTEPs involved in EVPN except for VSX nodes. In case of VSX VTEP (logical VTEP), the same `virtual-mac` must be configured in both the VSX peers. For ease of troubleshooting, it is also recommended to configure the same value of VSX `system MAC` in VSX VTEP (logical VTEP) peers.



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# vlan

```
vlan <ID>
no vlan <ID>
```

## Description

Specifies the VLAN ID and enters the VLAN context under EVPN.

The **no** form of this command removes this configuration.

| Parameter | Description                             |
|-----------|-----------------------------------------|
| <ID>      | Specifies the VLAN ID. Range: 2 - 4040. |

## Examples

```
switch(config-evpn)# vlan 10
switch(config-evpn-vlan-10)#
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context  | Authority                                                                          |
|---------------|------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan | Administrators or local user group members with execution rights for this command. |

# vlan-aware-bundle

```
vlan-aware-bundle<BUNDLE-NAME>
no vlan-aware-bundle<BUNDLE-NAME>
```

## Description

Creates the VLAN aware bundle instance and enters the VLAN Aware Bundle context.

The **no** form of this command removes this configuration.

| Parameter     | Description                       |
|---------------|-----------------------------------|
| <BUNDLE-NAME> | Represents the VLAN Aware Bundle. |

## Usage

VLAN aware bundle and VLAN based service can coexist, but the same VLAN/VNI cannot be part of the VLAN aware bundle and VLAN based service. The VLAN/VNI part of the VLAN aware bundle should be part of the VLAN aware bundle on all vteps.

## Examples

Creating the VLAN aware bundle instance bundle\_1 and entering the VLAN Aware Bundle context.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)#
```

Removing the VLAN aware bundle instance bundle\_1 and exiting the VLAN Aware Bundle context.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no vlan-aware-bundle bundle_1
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## vlan-ethernet-tag (evpn vlan-aware-bundles)

```
vlan-ethernet-tag <VLAN-ID> {ethernet tag}
no vlan-ethernet-tag <VLAN-ID> {ethernet tag}
```

### Description

Associates the Ethernet Tag ID value to VLANs of the VLAN aware bundles.

The **no** form of this command removes this configuration.

| Parameter      | Description                                                                 |
|----------------|-----------------------------------------------------------------------------|
| <VLAN-ID>      | Specifies the VLAN to which the ethernet tag is configuring. Range: 1-4094. |
| {ethernet tag} | Specifies the non-default ethernet tag for the VLAN. Range: 1-16777215.     |

### Usage

The Ethernet Tag ID value should be unique and associated to only one VLAN of the VLAN aware bundle. The configuration of this command is not mandatory, but may be required for interoperability with some third-party vendors.

### Examples

Associating the Ethernet tag ID value for vlan aware bundle bundle\_1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# vlan-ethernet-tag 10 20
```

Removing the Ethernet tag ID value for vlan aware bundle bundle\_1.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no vlan-ethernet-tag 10 20
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## vlan <ID-RANGE>

```
vlan <ID-RANGE>
no vlan <ID-RANGE>
```

### Description

Specifies the list of VLANs that are part of the VLAN Aware Bundle.  
The **no** form of this command removes this configuration.

| Parameter  | Description                                                     |
|------------|-----------------------------------------------------------------|
| <ID-RANGE> | Specifies the VLANS that are part of the bundle. Range: 1-4094. |

### Usage

If a VLAN is already part of VLAN based service, it cannot be configured under `vlan-aware-bundle` service and vice versa.

A VLAN cannot be part of more than one EVPN VLAN aware bundles.

### Examples

Creating the VLAN aware bundle instance bundle\_1 and entering the VLAN Aware Bundle context for vlan 5-10 and 15.



```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# vlan 5-10, 15
```

Removing the VLAN aware bundle instance bundle\_1 and exiting the VLAN Aware Bundle context for vlan 5-10 and 15.

```
switch(config-evpn)# vlan-aware-bundle bundle_1
switch(config-evpn-vlan-aware-bundle-bundle_1)# no vlan 5-10, 15
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-evpn-vlan-aware-bundle | Administrators or local user group members with execution rights for this command. |

## address

address {<IPV4-ADDR> | <IPV6-ADDR> | hostname <HOSTNAME>}  
no address {<IPV4-ADDR> | <IPV6-ADDR> | hostname <HOSTNAME>}

### Description

Specifies the NAS IP address or hostname.  
The **no** form of this command deletes an IP address or hostname.

| Parameter   | Description                                       |
|-------------|---------------------------------------------------|
| <IPV4-ADDR> | Specifies the NAS server IPv4 address, Global.    |
| <IPV6-ADDR> | Specifies the IPv6 address of the NAS server.     |
| <HOSTNAME>  | Specifies the hostname of the NAS server. String. |

### Examples

Creating the logfiles storage volume with IP address 10.1.1.1:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# address 10.1.1.1
```

Deleting an external storage volume named logfiles:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no address 10.1.1.1
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context                       | Authority                                                                          |
|---------------|---------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage-<VOLUME-NAME> | Administrators or local user group members with execution rights for this command. |

## directory

```
directory <DIRECTORY-NAME>
no directory <DIRECTORY-NAME>
```

### Description

Selects an existing directory on the external storage volume.

The **no** form of this command clears a directory of an external storage volume.

| Parameter        | Description                                                      |
|------------------|------------------------------------------------------------------|
| <DIRECTORY-NAME> | Specifies the external storage directory for mapping the volume. |

### Examples

Creating a volume named logfiles that is mapped under /home on the server:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# directory /home
```

Clearing the directory /home:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no directory /home
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context                       | Authority                                                                                                                                                              |
|---------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage-<VOLUME-NAME> | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# disable

disable  
no disable

## Description

Disables the external storage volume.

The **no** form of this command enables the external storage volume. This is identical to the `enable` command.

## Examples

Disabling a volume named logfiles:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# disable
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                     | Authority                                                                                                                                                              |
|---------------|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage- <i>&lt;VOLUME-NAME&gt;</i> | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# enable

enable  
no enable

## Description

Enables the external storage volume.

The **no** form of this command disables the external storage volume. This is identical to the `disable` command.

## Examples

Creating and then enabling a volume named logfiles:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# enable
```

Disables the external storage volume:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# disable
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                       | Authority                                                                                                                                                              |
|---------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage-<VOLUME-NAME> | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## external-storage

```
external-storage <VOLUME-NAME>
no external-storage <VOLUME-NAME>
```

### Description

Creates or updates an external storage volume.

The **no** form of this command deletes an external storage volume.

### Examples

Creating the logfiles storage volume:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)#
```

Deleting the logfiles storage volume:

```
switch(config)# no external-storage logfiles
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## password (external-storage)

```
password [{plaintext | ciphertext} <PASSWORD>]
no password {plaintext | ciphertext} <PASSWORD>
```

### Description

Sets the password for network attached storage server login.

The **no** form of this command clears the password for network attached storage server login.

| Parameter                | Description                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {ciphertext   plaintext} | Selects the password format.                                                                                                                                                                                           |
| <PASSWORD>               | Specifies the password.<br><br><b>NOTE:</b> When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks. |

### Examples

Creating a volume named logfiles with password Xj#9:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# password plaintext Xj#9
```

Creating a volume named bak1 with a prompted plaintext password:

```
switch(config)# external-storage bak1
switch(config-external-storage-bak1)# password
Enter the NAS server password: *****
Re-Enter the NAS server password: *****
```

Clearing the password for volume logfiles:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no password plaintext Xj#9
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                       | Authority                                                                          |
|---------------|---------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage-<VOLUME-NAME> | Administrators or local user group members with execution rights for this command. |

# show external-storage

show external-storage [<VOLUME-NAME>]

## Description

Shows external storage configuration and state for all volumes or for a specified volume.

| Parameter     | Description                                                                |
|---------------|----------------------------------------------------------------------------|
| <VOLUME-NAME> | Specifies the external storage volume name that the show command will use. |

## Examples

```
switch# show external-storage
```

```

--
 Address VRF Username Type Directory State

--
nfsvol 10.1.1.1 nas --- NFSv3 /home
operational
nfsfiles 20.1.1.1 nas netstorage NFSv4 /netstor disabled
scpdev nasserver nas scpstor SCP /scp
unaccessible
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show running-config external-storage

show running-config external-storage

### Description

Shows the running configuration of the external storage.

### Examples

```
switch# show running-config external-storage

external-storage nfsvol
 address 10.1.1.1
 vrf nas
 type nfsv4
 directoty /home
 enable
external-storage scpdev
 address 30.1.1.1
 vrf nas
 username switchuser
 password ciphertext xxx
 type scp
 directoty /home
 enable
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## type

```
type {nfsv3 | nfsv4 | scp}
no type {nfsv3 | nfsv4 | scp}
```



## Description

Sets the network attached storage access type for reaching the external storage volume. The **no** form of this command deletes an external storage volume.

| Parameter          | Description                                  |
|--------------------|----------------------------------------------|
| <code>nfsv3</code> | Specifies the NFSv3 network access protocol. |
| <code>nfsv4</code> | Specifies the NFSv4 network access protocol. |
| <code>scp</code>   | Specifies the SCP network access protocol.   |

## Examples

Creating the logfiles volume using NFSV4:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# type nfsv4
```

Clearing the external storage access type:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no type nfsv4
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                          | Authority                                                                          |
|---------------|----------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-external-storage-&lt;VOLUME-NAME&gt;</code> | Administrators or local user group members with execution rights for this command. |

## username

```
username <USER-NAME>
no username <USER-NAME>
```

## Description

Sets the username for logging in to a network attached storage server. The **no** form of this command clears a username.

| Parameter                      | Description             |
|--------------------------------|-------------------------|
| <code>&lt;USER-NAME&gt;</code> | Specifies the username. |

## Examples

Creating a volume named logfiles with the user name nassuser:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# username nasuser
```

Clearing the user name nasuser from accessing the logfiles volume:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no username nasuser
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                           | Authority                                                                          |
|---------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage- <code>&lt;VOLUME-NAME&gt;</code> | Administrators or local user group members with execution rights for this command. |

## vrf

```
vrf <VRF-NAME>
no vrf <VRF-NAME>
```

## Description

Setting a VRF to reach network attached storage.

The **no** form of this command clears access of a VRF to network attached storage.

| Parameter                     | Description             |
|-------------------------------|-------------------------|
| <code>&lt;VRF-NAME&gt;</code> | Specifies the VRF name. |

## Examples

Creating the logfiles volume and setting a VRF named nas to access the network attached storage:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# vrf nas
```

Clearing access of a VRF named nas to the network attached storage:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no vrf nas
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                     | Authority                                                                          |
|---------------|-----------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-external-storage- <i>&lt;VOLUME-NAME&gt;</i> | Administrators or local user group members with execution rights for this command. |

## erase feature-pack

erase feature-pack [reset]

### Description

Remove the installed feature pack and delete the feature pack file.

| Parameter | Description                                                                                                                                                                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| reset     | <i>Optional.</i> Include this parameter if you do not want to use subscription features anymore and want to stop receiving honor mode warning logs messages. <b>Running this command will disable all subscription features and stop honor warnings.</b> |

### Example

Remove the feature pack. The switch will continue to operate in honor mode.

```
switch# erase feature-pack
```

Remove the feature pack and disable all subscription features.

```
switch# erase feature-pack reset
```

This operation will delete the feature pack subscription key and reset feature pack enforcement to a factory default state. This will disable advanced features that require a subscription to operate and may impact network operation if those features are in use.

After running this command, advanced features can only be re-enabled through one of the following:

1. Installing a new feature-pack subscription key.
2. Connecting to HPE Aruba Networking Central.
3. Configuring honor mode.

Continue (y/n)?



For more information on features that use this command, refer to the Feature Pack Deployment Guide for your switch model.

### Command History

| Release | Modification                              |
|---------|-------------------------------------------|
| 10.14   | The <b>reset</b> parameter is introduced. |
| 10.13   | Command introduced.                       |

## Command Information

| Platforms     | Command context      | Authority                                                                          |
|---------------|----------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>manager</code> | Administrators or local user group members with execution rights for this command. |

## feature-pack mode

```
feature-pack mode
 cloud-managed
 file-based
 honor
 no ...
```

### Description

Set the operation mode for a feature pack deployment.

HPE Aruba Networking provides three modes for feature pack management: **cloud-managed**, **file-based**, and **honor**. In the event of a mismatch between the installed feature pack and the feature pack mode, the device will operate in honor mode.

| Parameter                  | Description                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------|
| <code>cloud-managed</code> | The device uses cloud-based feature pack management                                            |
| <code>file-managed</code>  | The device uses a manually installed feature pack file. This is the default feature pack mode. |
| <code>honor</code>         | A valid feature pack has been obtained, but is not yet installed.                              |
| <code>no ...</code>        | Resets the configuration back to the default file-based feature pack mode.                     |

### Usage

Switches using feature pack subscription keys in **cloud mode** share a pool of one or more feature pack subscription keys managed using the HPE Networking support portal. By default, a switch using an HPE Aruba Networking CX feature pack in cloud mode will contact the HPE Networking support portal once a day to automatically synchronize with the feature pack subscription key management database. With this deployment type, the HPE Networking support site can automatically distribute and manage feature packs for all devices in a group, making it a scalable solution for larger deployments and for global accounts across geographies.

Networks with a single switch, or with multiple switches on isolated networks that cannot contact the HPE Networking support site should use feature pack subscription keys in **file-based mode**, where a feature pack is manually enabled on a switch using a non-sharable subscription key tied to that individual switch's serial number or MAC address.

**Honor mode** is intended for cases where a valid feature pack for advanced features has been purchased, but is not yet installed on the device. Advanced features on this device will be operational in Honor mode, but a warning message may be seen until a valid feature pack is installed. Please note that HPE Aruba Networking will remove support for Honor mode in a future release and advanced features will only be operational if the applicable subscription fees are paid and a valid feature pack is installed.

## Examples

```
switch(config)# feature pack mode cloud-managed
```



For more information on features that use this command, refer to the Feature Pack Deployment Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## feature-pack server

```
feature-pack server
 block <block>
 credentials user <USER> password [{plaintext <PASSWORD>}|{ciphertext <PASSWORD>}]
 location <LOCATION> [vrf <VRF>]
 pool <pool>
```

## Description

If the switch is in cloud-managed feature pack mode, use this command to define the switch's feature pack profile. A switch in cloud-managed mode uses the information in this profile to contact the feature pack management server and download and install any allocated feature packs.

| Parameter     | Description                                                                                                                                         |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| block <block> | If the subscription pool for the profile contains more than one subscription block, specify the subscription block within that pool to be assigned. |
| credentials   | Configures the credentials used by the device to contact and authenticate to the feature pack server.                                               |

| Parameter                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>user &lt;USER&gt;</code>           | The user name of a feature pack server account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>password</code>                    | <p>Select a mode for entering the feature pack server password. If you press <b>&lt;enter&gt;</b> after the <b>password</b> parameter, you will enter a secure prompt that allows you to securely enter a hidden password. <i>This is the recommended method for entering a plaintext password.</i></p> <p>You can include the optional <b>plaintext</b> parameter to configure a plain text password (not recommended), or use the optional <b>ciphertext</b> parameter to enter previously encrypted ciphertext password.</p> |
| <code>plaintext &lt;PASSWORD&gt;</code>  | Optional. Enter a password in plain text without the secure prompt. <i>This option does not hide the password in the CLI, and is not recommended.</i>                                                                                                                                                                                                                                                                                                                                                                           |
| <code>ciphertext &lt;PASSWORD&gt;</code> | Optional. Enter a password as previously encrypted text. <i>This is the recommended method for entering an encrypted password.</i>                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>location &lt;LOCATION&gt;</code>   | The FQDN of the feature pack server;<br><code>https://cx-feature-pack.arubanetworks.com</code>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>[vrf &lt;VRF&gt;]</code>           | (Optional) Specify the VRF used to contact the feature pack server.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <code>pool &lt;pool&gt;</code>           | Configures the feature pack server subscription pool. This information is used by the feature pack server to properly identify the subscription to be assigned to the device.                                                                                                                                                                                                                                                                                                                                                   |

## Examples

Defining a feature pack server by entering a hidden plain text user password.

```
switch(config)# feature-pack server
switch(config-feature-pack-server)# location https://cx-feature-
pack.arubanetworks.com vrf mgmt
switch(config-feature-pack-server)# credentials user myLMSUser1234 password
Enter password: *****
Confirm password: *****
```

Defining a feature pack server with an encrypted ciphertext user password.

```
switch(config)# feature-pack server
switch(config-feature-pack-server)# location https://cx-feature-
pack.arubanetworks.com vrf mgmt
switch(config-feature-pack-server)# credentials user myLMSUser1234 password
ciphertext
AQBapcmUTsCVdaTGkLA3mN2sslLgsNOdqFUP0j+CaCxVdz7oEwAA2OmsmBmgPHavS+6Gkgm2twE4NU1Y=
```



For more information on features that use this command, refer to the Feature Pack Deployment Guide for your switch model.

## Command History

| Release    | Modification                                                                                                                                                                                                                                                                                            |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.13.1000 | Plaintext passwords should now be configured using the secure prompt, which can be accessed by pressing <enter> after the <b>password</b> keyword. This makes the <b>plaintext</b> and <b>ciphertext</b> keywords optional. It is recommended to use either the secure prompt or the ciphertext option. |
| 10.13      | Command introduced                                                                                                                                                                                                                                                                                      |

## Command Information

| Platforms     | Command context                      | Authority                                                                                                                                                              |
|---------------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>config-feature-pack-server | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# feature-pack validate

feature-pack validate

## Description

Manually trigger a feature pack validation on the HPE Networking support portal. (By default, automatic validation happens once every day.) This command is only applicable for feature packs in cloud-managed mode.

## Examples

```
switch# feature-pack validate
```



For more information on features that use this command, refer to the Feature Pack Deployment Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.13   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | manager         | Administrators or local user group members with execution rights for this command. |

# show feature-pack



```
show feature-pack [server]
```

## Description

Display the current feature pack summary and status, and feature status of features that require a feature pack.

| Parameter     | Description                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>server</i> | (Optional) For feature packs in cloud-managed mode, Include this parameter to display configuration settings used to connect to the feature pack management server, and display the connection status information. |

## Examples

```
switch# show feature-pack
Feature Pack Summary
=====
Name : CX Software Advanced Feature Pack
Expiration Date : Thu May 4 2025
Serial Number(s) : TW13KM304V
MAC Address : 90:20:c2:c4:98:00
Hostname : 6405
Mode : File based
Status : feature pack installed and valid
Error Reason : None

Feature Subscription Status Feature
----- -
Application Based Policy active allowed
MACsec extensions for WAN active allowed
Reflexive Policies for Port Access GBP Clients active allowed
Reflexive Policies for Port Access Clients active allowed
```

```
switch# switch# show feature-pack server
Profile
=====
Location URL : https://cx-feature-pack.arubanetworks.com
Location VRF : mgmt
User account : customer@example.com
Subscription Pool : default
Subscription Block : 6300_test_block_2
Connection
=====
Status : Validation success
Reason : --
Last validation time : Tue Sep 12 09:27:42 UTC 2023
Success validation time : Tue Sep 12 09:27:42 UTC 2023
```

The output of the **show feature-pack** command include the following information:

| Value           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name            | Name of the feature pack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Expiration Date | The date that the feature pack subscription expires                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Serial Numbers  | Serial numbers for that feature pack. If the feature pack is used by multiple switches (for example, in a VSF deployment) then the <b>Serial Number(s)</b> field displays all the switch serial numbers for that feature pack.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MAC address     | MAC address of the switch using the feature pack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Hostname        | Host name of the switch using the feature pack                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Type            | Shows the feature pack file type: <ul style="list-style-type: none"> <li>▪ <b>Device specific:</b> Feature pack was manually downloaded from a feature pack server account in local mode. Use this feature pack with a switch in file-based mode..</li> <li>▪ <b>Floating:</b> The feature pack was automatically downloaded from a cloud mode feature pack account on the HPE Networking support portal. This feature pack should be used with the switch in cloud-managed mode.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Mode            | Shows the feature pack configuration mode: <ul style="list-style-type: none"> <li>▪ <b>Cloud management:</b> Switches using feature pack subscriptions in cloud-managed mode share a pool of one or more feature pack subscriptions. These subscriptions are managed through the HPE Networking support portal.</li> <li>▪ <b>File Based:</b> If a switch is using a feature pack in <b>file-based mode</b>, you must manually upload the feature pack using the <b>copy</b> command and enable it on a switch using a non-sharable subscription file tied to that individual switch's serial number or MAC address.</li> <li>▪ <b>Honor:</b> Honor mode is intended for cases where a valid feature pack for advanced features has been purchased, but is not yet installed on the device. Advanced features on this device will be operational in honor mode, but a warning message may be seen until a valid feature pack is installed. Please note that HPE Aruba Networking will remove support for Honor mode in a future release and advanced features will only be operational if the applicable subscription fees are paid and a valid feature pack is installed. This message is shown when the switch is configured to use a cloud-managed feature pack profile using the <b>feature pack mode cloud-managed</b> command.</li> </ul> |
| Status          | This message displays the current status of the feature pack: <ul style="list-style-type: none"> <li>▪ <b>No feature pack installed:</b> No feature pack is detected on the switch.</li> <li>▪ <b>Feature pack installed and valid:</b> Feature pack installed with no errors.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Value

## Description

- **Feature pack install error:** The feature pack has invalid data.
- **Feature pack expired:** The feature pack subscription has expired.
- **Feature pack removed:** The feature pack was erased from the switch using the **erase** command.
- **Subscription through HPE Aruba Networking Central is connected:** Switch is actively connected to HPE Aruba Networking Central. Subscription features are operational. The feature-pack on the switch will display this state only if *all* the following are true:
  - The switch has a connection to HPE Aruba Networking Central.
  - The switch is onboarded to the GreenLake for PrivateCloud (GLPC) device inventory .
  - The switch is assigned to HPE Aruba Networking Central Application.
  - The switch has a valid HPE Aruba Networking Central License assigned.
- **Subscription through HPE Aruba Networking Central is disconnected:** Switch is disconnected from HPE Aruba Networking Central. Subscription features are still operational. The switch will appear in this state if any of the requirements for the status is not currently true, A switch may also display this feature pack status if the switch has connection to HPE Aruba Networking Central, is assigned to the Central application, but has no Central License attached. In this case the switch will be in disconnected state even if it never was previously in connected state.
- **Feature pack mode honor configured:** The switch does not have a valid feature pack. Subscription features are operational, and is operating in honor mode until the feature pack is installed.
- **Cloud managed server is disconnected:** The switch is managing feature packs in cloud mode, but the switch is no longer able to reach the HPE Networking support portal. The switch will continue to operate in honor mode.
- **Cloud managed and subscription revoked from server:** The switch is managing the feature pack in cloud mode, but feature pack has been revoked from the switch through the HPE Networking support portal. The switch will continue to operate in honor mode until the feature pack is removed from the switch.
- **Cloud managed server validation error:** Server validation failed. Issue the command **show feature pack server** for more information.
- **Unexpected VSF member in stack:** A feature pack intended

| Value               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <p>for a VSF stack is installed on a VSF member whose serial number is not covered under the current feature pack.</p> <ul style="list-style-type: none"> <li>▪ <b>Mode does not match installed feature pack type:</b> The feature pack type (device-locked or floating) does not match the configured mode. Device-locked feature packs should be used in file-based deployments only, and floating feature packs should be used by cloud-managed deployments.</li> </ul>                                                                                                                                                                         |
| Error Reason        | <p>If the feature pack <b>Status</b> field displays an error status, this field displays details about possible causes for the issue.</p> <ul style="list-style-type: none"> <li>▪ <b>Serial number mismatch:</b> The serial number in the installed feature pack does not match the switch's serial number.</li> <li>▪ <b>MAC address mismatch:</b> The MAC address in the installed feature pack does not match the switch's serial number.</li> <li>▪ <b>Feature pack file parsing error:</b> The feature pack file has an invalid format.</li> <li>▪ <b>Feature pack file signature invalid:</b> The feature pack file was modified.</li> </ul> |
| Feature             | Name of the feature supported by the feature pack.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Subscription Status | <p>Current subscription status;</p> <ul style="list-style-type: none"> <li>▪ <b>active:</b> Subscription is active.</li> <li>▪ <b>inactive:</b> Subscription is inactive or has expired.</li> <li>▪ <b>honor:</b> Installed feature pack has expired or cloud managed feature pack has encountered an error. Warnings will be logged periodically.</li> </ul>                                                                                                                                                                                                                                                                                       |
| Feature Pack Status | <p>Current status of the feature pack:</p> <ul style="list-style-type: none"> <li>▪ <b>allowed:</b> Feature is functional.</li> <li>▪ <b>blocked:</b> Feature is not functional and will require a valid feature pack to be functional.</li> <li>▪ <b>not running:</b> Feature is not configured on switch and daemon is not running</li> <li>▪ <b>unsupported on SKU:</b> Feature is not supported on product SKU.</li> <li>▪ <b>unsupported with VSF:</b> Feature is not supported on a VSF stack.</li> </ul>                                                                                                                                     |

The output of the **show feature-pack** server command include the following information:

|              |                                                                                                                                    |
|--------------|------------------------------------------------------------------------------------------------------------------------------------|
| Location URL | Fully qualified domain name of the feature pack subscription server, for example, <b>https://cx-feature-pack.arubanetworks.com</b> |
| Location VRF | VRF used to access the feature pack subscription server.                                                                           |
| User Account | User name of the user account at the HPE Networking support portal associated with the feature pack.                               |

|                         |                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subscription Pool       | Name of the subscription pool associated with the feature pack. This can be the <b>Default</b> subscription pool, or a user-defined subscription pool. |
| Subscription Block      | Subscription block associated with the feature pack.                                                                                                   |
| Status                  | Indicates whether the switch was able to contact the feature pack server.                                                                              |
| Reason                  | If the switch is unable to contact the feature pack server, this field can display information about the cause for the connection failure.             |
| Last validation time    | Timestamp showing the date and time the switch last contacted the feature pack server.                                                                 |
| Success Validation time | Timestamp showing the date and time of the last successful feature pack installation or validation against the feature pack server                     |



For more information on features that use this command, refer to the Feature Pack Deployment Guide for your switch model.

## Command History

| Release | Modification                                                                                                                                                                  |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.16   | The output of this command no longer displays the subscription status of the Application Recognition feature, as this feature no longer requires a feature pack subscription. |
| 10.13   | Command introduced                                                                                                                                                            |

## Command Information

| Platforms     | Command context      | Authority                                                                          |
|---------------|----------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>manager</code> | Administrators or local user group members with execution rights for this command. |

## fast-reroute

[no] fast-reroute

### Description

This command enables IP Fast Re-Route (IP-FRR) and is available in the router OSPF context.

| Parameter       | Description                       |
|-----------------|-----------------------------------|
| <code>no</code> | <i>Optional.</i> Disables IP-FRR. |



When IP FRR is enabled or disabled, there will be a momentary traffic loss for a few seconds since all the OSPF routes may get deleted and re-added as applicable.

## Examples

The following example shows how to enable IP fast-reroute for this OSPF instance:

```
switch(config)# router ospf 1
switch(config-ospf-1)# fast-reroute
switch(config-ospf-1)#
```

The following example shows how to disable IP-FRR:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no fast-reroute
switch(config-ospf-1)#
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-ospf-1   | Administrators or local user group members with execution rights for this command. |

## neighbor

neighbor <ipv4-address | ipv6-address | peer-group-name> fall-over bfd

### Description

The BGP Support for BFD enables BGP to register with Bidirectional Forwarding Detection (BFD) to receive fast peering session deactivation messages from BFD.

You can either configure BFD support for BGP per neighbor or peer-group. Multi-hop BFD is not supported for BGP.

| Parameter    | Description                                                  |
|--------------|--------------------------------------------------------------|
| ipv4-address | <i>Required.</i> The neighbor IP address.<br>Syntax: A.B.C.D |
| ipv6-address | <i>Required.</i> The neighbor IPv6 address.                  |

| Parameter       | Description                                               |
|-----------------|-----------------------------------------------------------|
|                 | Syntax:X:X::X:X                                           |
| peer-group-name | <i>Required.</i> Configure Peer-Group.<br>Syntax: PGNAME  |
| fall-over       | <i>Required.</i> Configure BGP session fast deactivation. |

## Example

The following example shows how configure BGP session fast deactivation and enable BFD for the BGP neighbor:

```
switch(config)# router bgp 1
switch(config-bgp)# neighbor 1.1.1.1 fall-over bfd
switch(config-bgp)# neighbor 1000::1 fall-over bfd
switch(config-bgp)# neighbor PG fall-over bfd
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-ospf-1   | Administrators or local user group members with execution rights for this command. |

# show capacities fast-reroute

show capacities fast-reroute

## Description

Displays the maximum number of Protected Nexthops configurable in a system.

## Example

The following example shows the maximum Protected Nexthop configurable in a system:

```
switch# show capacities fast-reroute
System Capacities: Filter Fast-Reroute
Capacities Name Value

Maximum number of Protected Nexthops configurable in a system 256
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show capacities status fast-reroute

show capacities-status fast-reroute

## Description

Displays the total number of Protected Nexthops currently configured on the device.

## Example

The following example shows the currently configured and the maximum Protected Nexthop in a system:

```
switch# show capacities-status fast-reroute

System Capacities Status: Filter Fast-Reroute
Capacities Name Value Maximum

Maximum number of Protected Nexthops currently configured 2 256
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |



### (Fault enabling/disabling)

```
{all | <FAULT>}
no {all | <FAULT>}
```

#### Description

Within the selected fault monitor profile context, enables all faults or specific faults for monitoring.



By default, all faults are disabled in a profile and remain disabled until enabled as described here. Configuring the action and threshold does not enable the fault.

Faults enabled with this command use default actions and thresholds unless the actions and thresholds are configured. For information on configuring actions and thresholds for a fault, respectively see [action](#) and [threshold](#).

The **no** form of this command disables faults for monitoring.

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all       | Selects all faults.                                                                                                                                                                                                                                                                                                                                        |
| <FAULT>   | Selects a specific fault. Available fault names:<br>excessive-broadcasts<br>excessive-multicasts<br>excessive-link-flaps<br>excessive-oversize-packets<br>excessive-jabbers<br>excessive-fragments<br>excessive-crc-errors<br>excessive-tx-drops<br>excessive-fc-watchdog-triggers (applies to HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series) |

#### Examples

Enabling all faults:

```
switch(config-fault-monitor-profile) # all
```

Disabling all faults:

```
switch(config-fault-monitor-profile)# no all
```

Enabling individual faults:

```
switch(config-fault-monitor-profile)# excessive-broadcasts
switch(config-fault-monitor-profile)# excessive-multicasts
switch(config-fault-monitor-profile)# excessive-link-flaps
switch(config-fault-monitor-profile)# excessive-oversize-packets
switch(config-fault-monitor-profile)# excessive-jabbers
switch(config-fault-monitor-profile)# excessive-fragments
switch(config-fault-monitor-profile)# excessive-crc-errors
switch(config-fault-monitor-profile)# excessive-tx-drops
switch(config-fault-monitor-profile)# excessive-fc-watchdog-triggers
```

Disabling individual faults:

```
switch(config-fault-monitor-profile)# no excessive-broadcasts
switch(config-fault-monitor-profile)# no excessive-multicasts
switch(config-fault-monitor-profile)# no excessive-link-flaps
switch(config-fault-monitor-profile)# no excessive-oversize-packets
switch(config-fault-monitor-profile)# no excessive-jabbers
switch(config-fault-monitor-profile)# no excessive-fragments
switch(config-fault-monitor-profile)# no excessive-crc-errors
switch(config-fault-monitor-profile)# no excessive-tx-drops
switch(config-fault-monitor-profile)# no excessive-fc-watchdog-triggers
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                              |
|------------|---------------------------------------------------------------------------|
| 10.12      | Added <b>excessive-fc-watchdog-triggers</b> on the 8325, 9300, and 10000. |
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000.               |

## Command Information

| Platforms     | Command context              | Authority                                                                          |
|---------------|------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-fault-monitor-profile | Administrators or local user group members with execution rights for this command. |

## action

```
{all | <FAULT>} action {notify | notify-and-disable [auto-enable <TIMEOUT>]}
```

```
no {all | <FAULT>} action {notify | notify-and-disable [auto-enable <TIMEOUT>]}
```

## Description

Within the selected fault monitor profile context, configures the fault monitoring action for the specified fault. Default action: **notify** with **auto-enable** disabled.

The no form of this command removes the action and disables **auto-enable**.

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all                   | Selects all faults.                                                                                                                                                                                                                                                                                                                                                                       |
| <FAULT>               | Selects a specific fault. Available fault names:<br>excessive-broadcasts<br>excessive-multicasts<br>excessive-link-flaps<br>excessive-oversize-packets<br>excessive-jabbers<br>excessive-fragments<br>excessive-crc-errors<br>excessive-tx-drops<br>excessive-alignment-errors<br>excessive-fc-watchdog-triggers (applies to HPE Aruba Networking 8325, 9300/9300S, 10000. Switch series) |
| notify                | Selects the <b>notify</b> action. Notifies through events, DLOGs, and SNMP trap. This action is enabled by default.                                                                                                                                                                                                                                                                       |
| notify-and-disable    | Selects the action as <b>notify-and-disable</b> . Notifies through events, DLOGs, and SNMP trap, and then disables the port.                                                                                                                                                                                                                                                              |
| auto-enable <TIMEOUT> | Sets the number of seconds after which a port disabled by the <b>notify-and-disable</b> action is automatically re-enabled. Range: 1 to 604800 seconds.                                                                                                                                                                                                                                   |



The fault parameter values are saved even after a fault is disabled in the profile. The saved values will be used if the fault is later re-enabled in the profile again.

## Examples

Configuring the **notify** action for all faults within a given profile:

```
switch(config-fault-monitor-profile)# all action notify
```

Configuring the **notify-and-disable** action for all faults within a given profile:

```
switch(config-fault-monitor-profile)# all action notify-and-disable
```

Configuring the **notify-and-disable** action for all faults with **auto-enable** within a given profile:

```
switch(config-fault-monitor-profile)# all action notify-and-disable auto-enable 80
```

Disabling all fault monitoring for this profile:

```
switch(config-fault-monitor-profile)# no all
```

Restoring all fault monitoring to the default action **notify** within a given profile:

```
switch(config-fault-monitor-profile)# no all action
```

Unconfiguring the auto-enable timer for all fault monitoring within a given profile:

```
switch(config-fault-monitor-profile)# no all action notify-and-disable auto-enable
```

Configuring the **notify** action for specific faults within a given profile:

```
switch(config-fault-monitor-profile)# excessive-oversize-packets action notify
switch(config-fault-monitor-profile)# excessive-fc-watchdog-triggers notify
```

Configuring the **notify-and-disable** action for specific faults within a given profile:

```
switch(config-fault-monitor-profile)# excessive-link-flaps action notify-and-disable
switch(config-fault-monitor-profile)# excessive-fragments action notify-and-disable
switch(config-fault-monitor-profile)# excessive-crc-errors action notify-and-disable
```

Configuring the **notify-and-disable** action with **auto-enable** for specific faults within a given profile:

```
switch(config-fault-monitor-profile)# excessive-broadcasts action notify-and-disable auto-enable 80
switch(config-fault-monitor-profile)# excessive-multicasts action notify-and-disable auto-enable 100
switch(config-fault-monitor-profile)# excessive-tx-drops action notify-and-disable auto-enable 70
switch(config-fault-monitor-profile)# excessive-jabbers action notify-and-disable auto-enable 60
```

Restoring fault monitoring to the default action **notify** within a given profile:

```
switch(config-fault-monitor-profile)# no excessive-fc-watchdog-triggers action
switch(config-fault-monitor-profile)# no excessive-oversize-packets action
switch(config-fault-monitor-profile)# no excessive-jabbers action
switch(config-fault-monitor-profile)# no excessive-oversize-packets action notify-and-disable
```

Unconfiguring the auto-enable timer within a given profile:

```
switch(config-fault-monitor-profile)# no excessive-jabbers action notify-and-disable auto-enable
```



---

For more information on features that use this command, refer to the Security Guide for your switch model.

---

## Command History

| Release    | Modification                                                              |
|------------|---------------------------------------------------------------------------|
| 10.12      | Added <b>excessive-fc-watchdog-triggers</b> on the 8325, 9300, and 10000. |
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000.               |

## Command Information

| Platforms     | Command context              | Authority                                                                          |
|---------------|------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-fault-monitor-profile | Administrators or local user group members with execution rights for this command. |

## apply fault-monitor profile

```
apply fault-monitor profile <PROFILE-NAME>
no apply fault-monitor profile [<PROFILE-NAME>]
```

### Description

Applies a fault monitoring profile to the selected interface or interface range.

The **no** form of this command removes the fault monitoring profile from the selected interface or interface range.

| Parameter      | Description                                                                                    |
|----------------|------------------------------------------------------------------------------------------------|
| <PROFILE-NAME> | Specifies the fault monitor profile name. Range: Up to 64 alphanumeric and special characters. |

### Examples

Applying the fault monitoring profile to a interface:

```
switch(config)# interface 1/1/1
switch(config-if)# apply fault-monitor profile noisy-ports
```

Applying the fault monitoring profile to a interface range:

```
switch(config)# interface 1/1/2-1/1/24
switch(config-if)# apply fault-monitor profile quiet-ports
```



For more information on features that use this command, refer to the Security Guide for your switch model.

### Command History

| Release    | Modification                                                |
|------------|-------------------------------------------------------------|
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## fault-monitor profile

```
fault-monitor profile <PROFILE-NAME>
no fault-monitor profile <PROFILE-NAME>
```

### Description

Creates a fault monitoring profile and enters its context which is indicated as **(config-fault-monitor-profile)**. If the profile already exists, this command enters the profile context. A maximum of 16 fault monitoring profiles are supported.

For information on enabling a fault within a fault monitor profile, see [\(Fault enabling/disabling\)](#).

For information on configuring actions and thresholds for a fault, respectively see [action](#) and [threshold](#).

For information on applying a fault monitor profile to a interface or interface range, see [apply fault-monitor profile](#).

The **no** form of this command deletes the fault monitoring profile.



By default, all faults are disabled in a profile.

| Parameter      | Description                                                                                    |
|----------------|------------------------------------------------------------------------------------------------|
| <PROFILE-NAME> | Specifies the fault monitor profile name. Range: Up to 64 alphanumeric and special characters. |

### Examples

Creating a fault monitor profile and entering its context:

```
switch(config)# fault-monitor profile noisy-ports
switch(config-fault-monitor-profile)#
```

Deleting a fault monitor profile:

```
switch(config)# no fault-monitor profile noisy-ports
```



For more information on features that use this command, refer to the Security Guide for your switch model.

### Command History

| Release    | Modification                                                |
|------------|-------------------------------------------------------------|
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000. |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show fault-monitor profile

show fault-monitor profile <PROFILE-NAME>

### Description

Shows fault monitoring profile information for all profiles or a specific profile.

| Parameter      | Description                                                                                    |
|----------------|------------------------------------------------------------------------------------------------|
| <PROFILE-NAME> | Specifies the fault monitor profile name. Range: Up to 64 alphanumeric and special characters. |

### Example

Showing information for all fault monitoring profiles:

```
switch# show fault-monitor profile

Fault monitor profile: noisy-ports

Auto
Fault Enabled Threshold Action Enable

excessive-broadcasts yes 5% notify-and-disable --
excessive-multicasts yes 1000 pps notify-and-disable --
excessive-link-flaps yes 7 notify-and-disable --
excessive-oversize-packets yes 25 notify-and-disable --
excessive-jabbers yes 25 notify-and-disable --
excessive-fragments yes 25 notify-and-disable --
excessive-crc-errors yes 25 notify-and-disable --
excessive-tx-drops yes 25 notify-and-disable --
excessive-fc-watchdog-triggers yes 1 notify-and-disable --

Fault monitor profile: quiet-ports

Auto
Fault Enabled Threshold Action Enable

excessive-broadcasts yes 20% notify-and-disable --
excessive-multicasts yes 25000 pps notify-and-disable 40
excessive-link-flaps yes 7 notify --
excessive-oversize-packets yes 30 notify-and-disable --
excessive-jabbers no 30 notify-and-disable 100
excessive-fragments yes 30 notify-and-disable --
excessive-crc-errors yes 30 notify-and-disable --
excessive-tx-drops yes 30 notify-and-disable --
excessive-fc-watchdog-triggers yes 25 notify-and-disable --
```

Showing information for a particular fault monitoring profile:

```
switch# show fault-monitor profile noisy-ports
```

```

Fault monitor profile: noisy-ports

```

```
Auto
Fault Enabled Threshold Action Enable

excessive-broadcasts yes 5% notify-and-disable --
excessive-multicasts yes 1000 pps notify-and-disable --
excessive-link-flaps yes 7 notify-and-disable --
excessive-oversize-packets yes 25 notify-and-disable --
excessive-jabbers yes 25 notify-and-disable --
excessive-fragments yes 25 notify-and-disable --
excessive-crc-errors yes 25 notify-and-disable --
excessive-tx-drops yes 25 notify-and-disable --
excessive-fc-watchdog-triggers yes 1 notify-and-disable --

```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                              |
|------------|---------------------------------------------------------------------------|
| 10.12      | Added <b>excessive-fc-watchdog-triggers</b> on the 8325, 9300, and 10000. |
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000.               |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show interface fault-monitor profile

```
show interface [<INTERFACE>|<IF-RANGE>] fault-monitor profile
```

### Description

Shows fault monitoring profile configuration information for all or specific interfaces.

| Parameter   | Description                   |
|-------------|-------------------------------|
| <INTERFACE> | Specifies a single interface. |
| <IF-RANGE>  | Specifies a interface range,  |

### Example

Showing all interfaces with applied fault monitoring profiles:



```
switch# show interface fault-monitor profile
```

| Port  | Fault Monitor Profile |
|-------|-----------------------|
| 1/1/1 | noisy-ports           |
| 1/1/2 | quiet-ports           |
| 1/1/4 | quiet-ports           |
| 1/1/5 | noisy-ports           |
| 1/1/6 | noisy-ports           |
| 1/1/7 | quiet-ports           |

Showing a range of interfaces with applied fault monitoring profiles:

```
switch# show interface 1/1/1-1/1/2,1/1/6 fault-monitor profile
```

| Port  | Fault Monitor Profile |
|-------|-----------------------|
| 1/1/1 | noisy-ports           |
| 1/1/2 | quiet-ports           |
| 1/1/6 | noisy-ports           |



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                |
|------------|-------------------------------------------------------------|
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show interface fault-monitor status

```
show interface [<INTERFACE>|<IF-RANGE>] fault-monitor status
```

## Description

Shows active fault information for all or specific interfaces.

| Parameter   | Description                   |
|-------------|-------------------------------|
| <INTERFACE> | Specifies a single interface. |
| <IF-RANGE>  | Specifies a interface range,  |

## Example

Showing active fault information for all interfaces with applied fault monitoring profiles:

```
switch# show interface fault-monitor status
```

| Port  | Fault                      | Fault Elapsed Time           | Port State | Time Left |
|-------|----------------------------|------------------------------|------------|-----------|
| 1/1/1 | excessive-broadcasts       | Tue Apr 14 14:29:09 UTC 2020 | down       | 60        |
|       | excessive-jabbers          | Tue Apr 15 14:29:09 UTC 2020 | --         | --        |
| 1/1/2 | excessive-oversize-packets | Tue Apr 16 14:29:09 UTC 2020 | down       | --        |

Showing active fault information for a range of interfaces with applied fault monitoring profiles:

```
switch# show interface 1/3/1,1/3/3 fault-monitor status
```

| Port  | Fault                | Occurring Since              | Port State | Time Left |
|-------|----------------------|------------------------------|------------|-----------|
| 1/1/4 | excessive-broadcasts | Tue Apr 14 14:29:09 UTC 2020 | down       | 60        |
|       | excessive-jabbers    | Tue Apr 15 14:29:09 UTC 2020 | --         | 100       |



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                |
|------------|-------------------------------------------------------------|
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show running-config

```
show running-config [interface <IFNAME> | current-context | all]
```

### Description

Shows the running configuration including any fault-monitor profile configurations and profile-names applied to an interface. The below examples focus on fault monitor-related configuration items. Other configuration items that may be present are represented by an ellipsis (. . .).

| Parameter          | Description                                                               |
|--------------------|---------------------------------------------------------------------------|
| interface <IFNAME> | Shows running configuration information for only the specified interface. |
| current-context    | Shows running configuration information for only the current context.     |
| all                | Shows all running configuration information.                              |

## Examples

Showing the running configuration for a particular interface:

```
switch# show running-config interface 1/1/1
interface 1/1/1
...
 apply fault-monitor profile noisy-ports
...
```

Showing the running configuration for a particular fault monitor profile current context:

```
switch# fault-monitor profile noisy-ports
switch(config-fault-monitor-profile)# show running-config current-context
fault-monitor profile noisy-ports
 excessive-broadcasts
 excessive-broadcasts threshold pps 10000
 excessive-broadcasts action notify-and-disable auto-enable 2000
 excessive-multicasts
 excessive-multicasts threshold pps 10000
 excessive-link-flaps
 excessive-link-flaps action notify-and-disable auto-enable 2000
```

Showing all running configuration:

```
switch# show running-config all
...
fault-monitor profile noisy-ports
 excessive-broadcasts
 excessive-broadcasts threshold pps 10000
 excessive-broadcasts action notify-and-disable auto-enable 2000
 excessive-multicasts
 excessive-multicasts threshold pps 10000
 excessive-multicasts action notify
 excessive-link-flaps
 excessive-link-flaps threshold count 7
 excessive-link-flaps action notify-and-disable auto-enable 2000
 no excessive-oversize-packets
 excessive-oversize-packets threshold value 25
 excessive-oversize-packets action notify
 no excessive-jabbers
 excessive-jabbers threshold value 25
 excessive-jabbers action notify
 no excessive-fragments
 excessive-fragments threshold value 25
 excessive-fragments action notify
 no excessive-crc-errors
 excessive-crc-errors threshold value 25
 excessive-crc-errors action notify
 no excessive-tx-drops
 excessive-tx-drops threshold value 25
 excessive-tx-drops action notify
 excessive-fc-watchdog-triggers
 excessive-fc-watchdog-triggers threshold count 1
 excessive-fc-watchdog-triggers action notify-and-disable
...
interface 1/1/1
...
 apply fault-monitor profile noisy-ports
```

...



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                              |
|------------|---------------------------------------------------------------------------|
| 10.12      | Added <b>excessive-fc-watchdog-triggers</b> on the 8325, 9300, and 10000. |
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000.               |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## threshold

```
<FAULT> threshold value <VALUE>
no <FAULT> threshold [value <VALUE>]
```

```
excessive-link-flaps threshold count <COUNT>
no excessive-link-flaps threshold [count <COUNT>]
```

```
excessive-fc-watchdog-triggers threshold count <COUNT>
no excessive-fc-watchdog-triggers threshold [count <COUNT>]
```

```
{excessive-broadcasts | excessive-multicasts}
 threshold {percent <BW-PERCENT> | pps <PPS>}
no {excessive-broadcasts | excessive-multicasts}
 threshold [{percent <BW-PERCENT> | pps <PPS>}]
```

```
no all threshold
```

## Description

Within the selected fault monitor profile context, sets the specified fault threshold.

The **no** form of this command resets the threshold to its default value.

| Parameter                                                                                                                                                                   | Description                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;FAULT&gt; threshold value &lt;VALUE&gt;</code>                                                                                                                    | Sets the threshold number of bad frames per 10000 good frames received or per 10000 good frames sent (depending on the fault), to be considered a fault. Range: 1 to 10000. Default: 25. |
| With <code>&lt;FAULT&gt;</code> set to any of these names:<br><code>excessive-oversize-packets</code><br><code>excessive-jabbers</code><br><code>excessive-fragments</code> |                                                                                                                                                                                          |

| Parameter                                                                          | Description                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| excessive-crc-errors<br>excessive-tx-drops                                         |                                                                                                                                                                                                                                                                                   |
| excessive-link-flaps<br>threshold count <COUNT>                                    | Sets the threshold count of interface link flaps, during a 10 second sampling interval, to be considered a fault. Range: 1 to 100. Default: 7.                                                                                                                                    |
| excessive-fc-watchdog-triggers<br>threshold count <COUNT>                          | (Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch Series.)<br>Sets the fault threshold as a count of the minimum number of flow-control watchdog triggers within a 20-second sampling interval that is considered to be a fault. Range: 1 to 10000. Default: 1. |
| {excessive-broadcasts  <br>excessive-multicasts}<br>threshold percent <BW-PERCENT> | Sets the fault threshold as a percentage of port bandwidth for minimum sized packets that is considered to be a fault. Range: 1 to 100. Default 5.                                                                                                                                |
| {excessive-broadcasts  <br>excessive-multicasts}<br>threshold pps <PPS>            | Sets the fault threshold in packets per second. Range: 1 to 195312500.                                                                                                                                                                                                            |

If excessive-broadcast or excessive-multicast faults are configured with the threshold higher than the `rate-limit` threshold, the following occurs:

- Fault reporting still happens as the port has actually received packets at a rate that violated its threshold.
- Traffic gets shaped as per `rate-limit` configuration and any packet exceeding the `rate-limit` threshold gets dropped.

## Examples

Setting thresholds:

```
switch(config-fault-monitor-profile)# excessive-oversize-packets threshold value 40
switch(config-fault-monitor-profile)# excessive-jabbers threshold value 30
switch(config-fault-monitor-profile)# excessive-fragments threshold value 50
switch(config-fault-monitor-profile)# excessive-crc-errors threshold value 35
switch(config-fault-monitor-profile)# excessive-tx-drops threshold value 20

switch(config-fault-monitor-profile)# excessive-link-flaps threshold count 14
switch(config-fault-monitor-profile)# excessive-fc-watchdog-triggers threshold count 5
switch(config-fault-monitor-profile)# excessive-broadcasts threshold percent 40
switch(config-fault-monitor-profile)# excessive-multicasts threshold pps 7500
```

Resetting all thresholds to their defaults:

```
switch(config-fault-monitor-profile)# no all threshold
```

Resetting individual thresholds to their defaults:

```

switch(config-fault-monitor-profile) # no excessive-oversize-packets threshold
switch(config-fault-monitor-profile) # no excessive-jabbers threshold
switch(config-fault-monitor-profile) # no excessive-fragments threshold
switch(config-fault-monitor-profile) # no excessive-crc-errors threshold
switch(config-fault-monitor-profile) # no excessive-tx-drops threshold

switch(config-fault-monitor-profile) # no excessive-link-flaps threshold
switch(config-fault-monitor-profile) # no excessive-fc-watchdog-triggers threshold

switch(config-fault-monitor-profile) # no excessive-broadcasts threshold
switch(config-fault-monitor-profile) # no excessive-multicasts threshold

```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                              |
|------------|---------------------------------------------------------------------------|
| 10.12      | Added <b>excessive-fc-watchdog-triggers</b> on the 8325, 9300, and 10000. |
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000.               |

## Command Information

| Platforms     | Command context              | Authority                                                                          |
|---------------|------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-fault-monitor-profile | Administrators or local user group members with execution rights for this command. |

## vsx-sync (fault monitor)

```

vsx-sync
no vsx-sync

```

### Description

Within the selected fault monitor profile context, configures VSX synchronization for the selected fault monitoring profile.

The **no** form of this command removes the VSX synchronization for a fault monitoring profile.

### Example

Configuring VSX synchronization for a fault monitoring profile:

```

switch(config-fault-monitor-profile) # vsx-sync

```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                |
|------------|-------------------------------------------------------------|
| 10.11.1000 | Command introduced on the 8320, 8325, 8360, 9300 and 10000. |

## Command Information

| Platforms     | Command context                           | Authority                                                                          |
|---------------|-------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-fault-monitor-profile</code> | Administrators or local user group members with execution rights for this command. |

**copy {primary | secondary} <REMOTE-URL>**

```
copy {primary | secondary} <REMOTE-URL> [vrf <VRF-NAME>]
```

**Description**

Uploads a firmware image to a TFTP or SFTP server.

| Parameter             | Description                                                                                                                                                                                                                                                                                                            |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {primary   secondary} | Selects the primary or secondary image profile to upload.<br>Required                                                                                                                                                                                                                                                  |
| <REMOTE-URL>          | Specifies the URL to receive the uploaded firmware using SFTP ,<br>TFTP or SCP.<br><b>TFTP format:</b><br>tftp://<IP-ADDR>[:<PORT-NUM>]<br>[;blocksize=<Value>]/<FILENAME><br><b>SFTP format:</b><br>sftp://<USERNAME>@<IP-ADDR><br>[:<PORT-NUM>]/<FILENAME><br><b>SCP format:</b><br>scp://USER@{IP HOST}[:PORT]/FILE |
| vrf <VRF-NAME>        | Specifies a VRF name. Default: default.                                                                                                                                                                                                                                                                                |

**Examples**

TFTP upload:

```
switch# copy primary tftp://192.0.2.0/00_10_00_0002.swi
100.0%
Verifying and writing system firmware...
```

SFTP upload:

```
switch# copy primary sftp://swuser@192.0.2.0/00_10_00_0002.swi
swuser@192.0.2.0's password:
Connected to 192.0.2.0.
sftp> put primary.swi XL_10_00_0002.swi
Uploading primary.swi to /users/swuser/00_10_00_0002.swi
primary.swi 100% 179MB 35.8MB/s 00:05
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.



## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy {primary | secondary} <FIRMWARE-FILENAME>

copy {primary | secondary} <FIRMWARE-FILENAME>

### Description

Copies a firmware image to USB storage.

| Parameter             | Description                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {primary   secondary} | Selects the primary or secondary image from which to copy the firmware. Required                                                                                                                                                                                  |
| <FIRMWARE-FILENAME>   | Specifies the name of the firmware file to create on the USB storage device. Prefix the filename with <b>usb:/</b> . For example:<br><b>usb:/firmware_v1.2.3.swi</b><br>For information on how to format the path to a firmware file on a USB drive, see USB URL. |

## Examples

```
switch# copy primary usb:/11.10.00.0002.swi
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy primary secondary

copy primary secondary

## Description

Copies the firmware image from the primary to the secondary location.

## Examples

```
switch# copy primary secondary
The secondary image will be deleted.

Continue (y/n)? y
Verifying and writing system firmware...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy <REMOTE-URL>

copy <REMOTE-URL> {hot-patch|primary|secondary} [vrf <VRF-NAME>]

## Description

Downloads a hot-patch or firmware image from a TFTP or SFTP server.

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <REMOTE-URL> | <p>Specifies the URL from which to download the firmware using SFTP or TFTP.</p> <p><b>TFTP format:</b></p> <pre>tftp://&lt;IP-ADDR&gt;[:&lt;PORT-NUM&gt;] [;blocksize=&lt;Value&gt;]/&lt;FILENAME&gt;</pre> <p><b>SFTP format:</b></p> <pre>sftp://&lt;USERNAME&gt;@&lt;IP-ADDR&gt; [:&lt;PORT-NUM&gt;]/&lt;FILENAME&gt;</pre> <p><b>SCP format:</b></p> <pre>scp://USER@{IP HOST}[:PORT]/FILE</pre> |

| Parameter                                  | Description                                                                                                                                                                                           |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>{hot-patch primary secondary}</code> | Select a hot-patch or a primary or secondary image profile for receiving the downloaded firmware. Required.<br><br><b>NOTE:</b> For more information about hot-patch, see <a href="#">hot-patch</a> . |
| <code>vrf &lt;VRF-NAME&gt;</code>          | Specifies the name of a VRF. Default: default.                                                                                                                                                        |

## TFTP usage

To specify a URL with:

- an IPv4 address: **tftp://192.0.2.1/a.txt**
- an IPv6 address: **tftp://[2000::2]/a.txt**
- a hostname: **tftp://hpe.com/a.txt**

To specify TFTP with:

- the port number of the server in the URL: **tftp://192.0.2.1:12/a.txt**
- the blocksize in the URL: **tftp://192.0.2.1;blocksize=1462/a.txt**

The valid blocksize range is 8 to 65464.

- the port number of the server and blocksize in the URL: **tftp://192.0.2.1:12;blocksize=1462/a.txt**

To specify a file in a directory of URL: **tftp://192.0.2.1/dir/a.txt**

## SFTP usage

To specify:

- A URL with an IPv4 address: **sftp://user@192.0.2.1/a.txt**
- A URL with an IPv6 address: **sftp://user@[2000::2]/a.txt**
- A URL with a hostname: **sftp://user@hpe.com/a.txt**
- SFTP port number of a server in the URL: **sftp://user@192.0.2.1:12/a.txt**
- A file in a directory of URL: **sftp://user@192.0.2.1/dir/a.txt**
- To specify a file with absolute path in the URL: **sftp://user@192.0.2.1//home/user/a.txt**

## SCP Usage

To specify:

- A username with an IP address: **scp://user@192.0.2.1:12/a.txt**
- A username with a remote host: **scp://user@hpe.com/a.txt**

## Examples

TFTP download for a hot-patch:

```
switch# copy tftp://192.168.1.1/FL.10.12.0001-0002.patch hot-patch vrf vrf1

Fetching /users/swuser/FL.10.10.0001-0002.patch to hotpatch.dnld.uE2YT1
FL.10.12.0001-0002.patch 100% 62KB 12.4MB/s 00:00
```

```
Verifying and writing hot-patch...
```

TFTP download for primary software image:

```
switch# copy tftp://192.10.12.0/FL_10_12_0001.swi primary
The primary image will be deleted.

Continue (y/n)? y
100.0%
Verifying and writing system firmware...
```

SFTP download:

```
switch# copy sftp://swuser@192.10.12.0/FL_10_12_0001.swi primary
The primary image will be deleted.

Continue (y/n)? y
The authenticity of host '192.10.12.0 (192.10.12.0)' can't be established.
ECDSA key fingerprint is SHA256:L64khLwlyLgXlARKRMiwcAAK8oRaQ8C0oWP+PkGBXHY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.10.12.0' (ECDSA) to the list of known hosts.
swuser@192.10.12.0's password:
Connected to 192.10.12.0.
Fetching /users/swuser/ss.10.00.0002.swi to ss.10.00.0002.swi.dnld
/users/swuser/ss.10.00.0002.swi 100% 179MB 25.6MB/s 00:07
Verifying and writing system firmware...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                        |
|------------------|---------------------------------------------------------------------|
| 10.12            | The <code>hot-patch</code> parameter is supported on all platforms. |
| 10.07 or earlier | --                                                                  |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy secondary primary

copy secondary primary

### Description

Copies the firmware image from the secondary to the primary location.

## Examples

```
switch# copy secondary primary
The primary image will be deleted.

Continue (y/n)? y
Verifying and writing system firmware...
```

```
switch# copy sftp://stor@192.22.1.0/im-switch.swi primary vrf mgmt
The primary image will be deleted.

Continue (y/n)? y
The authenticity of host '192.22.1.0 (192.22.1.0)' can't be established.
ECDSA key fingerprint is SHA256:MyI1xbdKnehYut0NLfL69gDpNzCmZqBVvBaRR46m7o8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.22.1.0' (ECDSA) to the list of known hosts.
stor@192.22.1.0's password:
Connected to 192.22.1.0.
sftp> get c8d5b9f-topflite.swi c8d5b9f-topflite.swi.dnld
Fetching /home/dr/im-switch.swi to c8d5b9f-topflite.swi.dnld
/home/dr/im-switch.swi 100% 226MB 56.6MB/s 00:04

Verifying and writing system firmware...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy <STORAGE-URL>

copy <STORAGE-URL> {hot-patch|primary|secondary}

### Description

Copies, verifies, and installs a hot-patch or firmware image from a USB storage device connected to the active management module.

| Parameter     | Description                                                      |
|---------------|------------------------------------------------------------------|
| <STORAGE-URL> | Specifies the name of the firmware file to copy from the storage |

| Parameter                                  | Description                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | device. Required.<br><b>USB format:</b><br><code>usb: /&lt;FILENAME&gt;</code>                                                                                                          |
| <code>{hot-patch primary secondary}</code> | Select a hot-patch image or a primary or secondary profile for receiving the copied firmware.<br><br><b>NOTE:</b> For more information about hot-patch, see <a href="#">hot-patch</a> . |

## USB usage

To specify a file:

- In a USB storage device: **usb:/a.txt**
- In a directory of a USB storage device: **usb:/dir/a.txt**

## Examples

```
switch# copy usb:/FL.10.12.0001-0002.patch
```

```
switch# copy usb:/FL.10.12.0001.swi primary
The primary image will be deleted.

Continue (y/n)? y

Verifying and writing system firmware...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                           |
|------------------|--------------------------------------------------------|
| 10.12            | The hot-patch parameter is supported on all platforms. |
| 10.07 or earlier | --                                                     |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy hot-patch

```
copy hot-patch <Word> {<REMOTE-URL>|<Storage-URL>} [vrf <VRF-NAME>]
```

## Description

Copies a hot-patch from a switch to the specified remote URL or storage URL.

| Parameter                         | Description                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;Word&gt;</code>         | Name of the hot-patch software to upload.                                                                                                                                      |
| <code>&lt;REMOTE-URL&gt;</code>   | Specifies the URL to receive the uploaded patch using SFTP or TFTP. For information on how to format the remote URL, see URL formatting for copy commands.                     |
| <code>vrf &lt;VRF-NAME&gt;</code> | [Optional] specify the VRF instance to use for upload.                                                                                                                         |
| <code>&lt;STORAGE-URL&gt;</code>  | Specifies the name of the patch file to create on the USB storage device. Prefix the filename with <b>usb:/</b> , for example, <b>usb:/firmware_FL_10_12_0001-0002.patch</b> . |

## Examples

```
switch# copy hot-patch FL_10_12_0001-0002.patch tftp:172.21.18.170/FL_10_12_0001-0002.patch vrf vrf1
```

## Related Commands

| Command                                 | Description                                             |
|-----------------------------------------|---------------------------------------------------------|
| <a href="#">copy &lt;REMOTE-URL&gt;</a> | Downloads a hot-patch image from a TFTP or SFTP server. |
| <a href="#">hot-patch</a>               | Apply a hot-patch image or remove it from the switch.   |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                                 |
|---------|----------------------------------------------|
| 10.12   | Hot-patch is now supported on all platforms. |
| 10.10   | Command introduced                           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## hot-patch

```
hot-patch apply|remove <name.patch>
no hot-patch apply <name.patch>
```

## Description

Apply hot-patch software or remove it from the switch. The **no** form of the **hot-patch apply** command disables the hot-patch image, but does not remove it from the switch. Rebooting the system after disabling or removing the patch is not required.

| Profile names                          | Description                                                                                                                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>apply &lt;name.patch&gt;</code>  | Apply the specified hot-patch image to a standalone switch or VSF stack. AOS-CX hot-patch software images can be obtained from HPE Aruba Networking customer support, and are identified with a <b>.patch</b> extension. |
| <code>remove &lt;name.patch&gt;</code> | Disables the hot-patch image and removes the patch from the switch. This removal will also disable the patch. Once removed, a hot-patch must be downloaded again in order to be applied.                                 |

## Usage

A hot-patch can be downloaded from a remote server onto a switch then applied without rebooting the switch. When the hot-patch is disabled, the hot-patch will still remain on the system. The disabled hot-patch can be removed from the system without the need for a reboot of the system.

If a checkpoint configuration that does not contain a hot-patch is restored to a running configuration that does have a hot-patch, the patch is not deleted, it remains as not applied but is present in the device memory.

## Examples

```
switch(config)# hot-patch apply FL_10_12_0001-0002.patch
```

## Related Commands

| Command                                              | Description                                                                               |
|------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <a href="#"><code>copy &lt;REMOTE-URL&gt;</code></a> | Downloads and installs a hot-patch image from a TFTP or SFTP server.                      |
| <a href="#"><code>copy hot-patch</code></a>          | Copies a hot-patch software image from a switch to a specified remote URL or storage URL. |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                                 |
|---------|----------------------------------------------|
| 10.12   | Hot-patch is now supported on all platforms. |
| 10.10   | Command introduced.                          |



## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show hot-patch

show hot-patch [detail]

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| detail    | Displays the detailed status of all hot-patches present on the system. |

### Description

the **show hot-patch** command displays the status of all hot-patches present on the system. The **show hot-patch detail** command displays detailed information for all hot patches present on the system.

### Examples

```
switch# show hot-patch

Name Status

FL_10_12_0001-0002.patch Applied

switch# show hot-patch detail

Name : FL_10_12_0001-0002.patch
Status : Applied
Version : FL_10_12_0001-0002.patch
Compatible Version : FL.10.12.0001
Issues Fixed : CR1234, CR2345
Patch Date : 2022-03-29 20:46:15 UTC
Patch ID : AOS-CX:FL.10.12.0001-sp1-256-gd457e88d39:20220442009
Patch SHA : a4038d06a2e5fe7e0d457e868d39e526185b
```

### Related Commands

| Command                                 | Description                                             |
|-----------------------------------------|---------------------------------------------------------|
| <a href="#">copy &lt;REMOTE-URL&gt;</a> | Downloads a hot-patch image from a TFTP or SFTP server. |
| <a href="#">hot-patch</a>               | Apply a hot-patch image or remove it from the switch.   |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification                              |
|---------|-------------------------------------------|
| 10.12   | Command supported on all platforms.       |
| 10.10   | Command introduced on 6300 Switch series. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# Flow monitoring commands

## diag-dump ipfix basic

diag-dump ipfix basic

### Description

Displays diagnostic information for IPFIX.

### Examples

```
diag-dump ipfix basic
=====
[Start] Feature ipfix Time : Tue Apr 11 02:23:03 2023
=====

[Start] Daemon ipfixd

- IPFIX Record Cache dump -
- IPFIX Record ipfix -

....

:- IPFIX Monitor v6ti completed -
- End of IPFIX Monitor Cache dump -

[End] Daemon ipfixd

[Start] Daemon ops-switchd

Key format: <traffic_type>_<coalescence_id>_<agent_id>_<asic_port>
Key TCAM Entry ID Count

1_1532781829_3_20 0xfffff7c7e7a00 1
1_3217499901_1_12 0xfffff91187580 1
1_3217499901_1_13 0xfffff91183d80 1
1_3217499901_1_14 0xfffff91186e80 1

....

[End] Daemon ops-switchd
```

```

=====
```

[End] Feature ipfix

```
=====
```

Diagnostic-dump captured for feature ipfix



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification                                       |
|---------|----------------------------------------------------|
| 10.15   | Command introduced on 9300S and 6200 Switch series |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## description

```
description <DESCRIPTION>
no description <DESCRIPTION>
```

## Description

Configures the description for the following telemetry options:

- flow monitor in the **config-flow-monitor** context
- flow congestion monitor in the **config-flow-congestion-monitor** context
- flow exporter in the **config-flow-exporter** context
- flow record in the **config-flow-record** context

The no form deletes a flow congestion monitor.

| Parameter     | Description                                                     |
|---------------|-----------------------------------------------------------------|
| <DESCRIPTION> | Displays a string of 256 characters, maximum, including spaces. |

## Examples

Adding or modifying the description of flow monitor, **flow-monitor-1**:

```
switch(config)# flow monitor flow-monitor-1
switch(config-flow-monitor)# description Used for analyzing basic ipv4 traffic
```

Adding or modifying the description of flow record, **flow-record-1**:

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# description Used for basic traffic analysis
```

Adding or modifying the description of flow exporter, **flow-exporter-1**:

```
switch(config)# flow exporter flow-exporter-1
```

```
switch(config-flow-exporter)# description Exports flows to 10.2.3.45:2055
```

Removing the description of flow monitor, **flow-monitor-1**:

```
switch(config)# flow exporter flow-monitor-1
switch(config-flow-exporter)# no description
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context                                                                                     | Authority                                                                          |
|---------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-flow-record<br>config-flow-monitor<br>config-flow-congestion-monitor<br>config-flow-exporter | Administrators or local user group members with execution rights for this command. |

## exporter

```
exporter <EXPORTER-NAME>
no exporter <EXPORTER-NAME>
```

## Description

Assigns a flow exporter to **flow monitor** in the **config-flow-monitor** context and **flow congestion monitor** in the **config-flow-congestion-monitor** context.

The no form removes the flow exporter from the selected monitor.

| Parameter       | Description                                                      |
|-----------------|------------------------------------------------------------------|
| <EXPORTER-NAME> | Specifies the name of the flow exporter assigned to the monitor. |



A maximum of one flow exporter can be applied to each flow monitor, and one flow exporter can be applied to each flow congestion monitor.

## Examples

Assigning flow exporter, **flow-exporter-1**, to flow monitor, **flow-monitor-1**:

```
switch(config)# flow monitor flow-monitor-1
switch(config-flow-monitor)# exporter flow-exporter-1
```

Removing a flow exporter assigned to flow monitor, **flow-monitor-1**:

```
switch(config)# flow monitor flow-monitor-1
switch(config-flow-monitor)# no exporter flow-exporter-1
```

Attempting to assign non-existent flow exporter, **flow-exporter-5**, to flow monitor, **flow-monitor-1**:

```
switch(config)# flow monitor flow-monitor-1
switch(config-flow-monitor)# exporter flow-exporter-5
Flow exporter 'flow-exporter-5' does not exist.
switch(config-flow-monitor)#
```

Assigning flow exporter, **flow-exporter-1**, to flow congestion monitor, **congestion-monitor-1**:

```
switch(config)# flow congestion-monitor congestion-monitor-1
switch(config-flow-congestion-monitor)# exporter flow-exporter-1
```

Removing a flow exporter assigned to flow congestion monitor:

```
switch(config)# flow congestion-monitor congestion-monitor-1
switch(config-flow-congestion-monitor)# no exporter flow-exporter-1
```

Attempting to assign non-existent flow exporter, **flow-exporter-5**, to flow congestion monitor, **congestion-monitor-1**:

```
switch(config)# flow congestion-monitor congestion-monitor-1
switch(config-flow-congestion-monitor)# exporter flow-exporter-5
Flow exporter 'flow-exporter-5' does not exist.
switch(config-flow-congestion-monitor)#
```

Attempting to assign flow exporter, **flow-exporter-6**, to monitor, **flow-monitor-3**, when two exporters are assigned:

```

switch(config)# flow monitor flow-monitor-3
switch(config-flow-monitor)# exporter flow-exporter 4
switch(config-flow-monitor)# exporter flow-exporter 5
switch(config-flow-monitor)# exporter flow-exporter 6
Cannot assign more than two flow exporters to a flow monitor.
switch(config-flow-monitor)#

```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms | Command context                | Authority                                                                          |
|-----------|--------------------------------|------------------------------------------------------------------------------------|
| 9300      | config-flow-monitor            | Administrators or local user group members with execution rights for this command. |
| 9300S     | config-flow-congestion-monitor |                                                                                    |

## flow exporter

```

flow exporter <name>
 description <description>
 destination
 <hostname>
 [vrf <vrfname>]
 <ipaddr>
 [vrf <vrfname>]
 <ip6addr>
 [vrf <vrfname>]
 type
 hostname-or-ip-addr
 traffic-insight}
 traffic-insight <instance-name>
no ...
template data timeout <timeout>
transport udp <port>

```

## Description

A flow exporter is the part of the IP Flow Information Export (IPFIX) feature that defines how a flow monitor exports flow reports. You can assign the same flow exporter configuration to more than one flow monitor. Each flow exporter includes a destination setting that identifies the device to which the flow reports are sent

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <name>                          | Name of the flow exporter, up to 64 characters.                                                                                                                                                                                                                                                                                     |
| description <description>       | A description of the flow exporter, up to 256 characters and spaces.                                                                                                                                                                                                                                                                |
| destination                     | Configure the export destination                                                                                                                                                                                                                                                                                                    |
| <hostname>                      | The exporter sends flow records to the specified hostname destination. The hostname can be a string of up to 64 characters.                                                                                                                                                                                                         |
| <IPaddr>                        | The exporter sends flow records to this IPv4 address destination.                                                                                                                                                                                                                                                                   |
| <ip6addr>                       | The exporter sends flow records to this IPv6 address destination.                                                                                                                                                                                                                                                                   |
| vrf <vrfname>                   | You can optionally include the name of the destination VRF in the destination definition on 5420, 6200, 6300, 6400, 8100, 8360, 9300S Switch series.                                                                                                                                                                                |
| type                            | Configure the type of the destination.                                                                                                                                                                                                                                                                                              |
| hostname-or-ip-addr             | Define the destination type as a hostname or IP address.                                                                                                                                                                                                                                                                            |
| traffic-insight <name>          | Define the destination type as a traffic insight instance.                                                                                                                                                                                                                                                                          |
| no ...                          | Negate any configured parameter.                                                                                                                                                                                                                                                                                                    |
| traffic-insight <INSTANCE-NAME> | Specify the a Traffic Insight instance to be used as the destination.                                                                                                                                                                                                                                                               |
| template data timeout <timeout> | A flow exporter template describes the format of exported flow reports. Therefore, flow reports cannot be decoded properly without the corresponding templates. This setting defines how often the flow exporter will resend templates to the flow monitor. The supported range is 1-86400 seconds, and the default is 600 seconds. |
| transport udp <port>            | Transport protocol and port for sending flow record reports. The default port is port 4739.                                                                                                                                                                                                                                         |

## Usage

The following table shows the maximum supported of flow monitors and flow exporters for each switch model.

| Switch        | Maximum Flow Monitors | Maximum Flow Exporters                                |
|---------------|-----------------------|-------------------------------------------------------|
| 9300<br>9300S | 1                     | One flow exporter can be applied to the flow monitor. |

## Examples

The following example creates a flow exporter configuration named **exporter-1**.

```
switch(config)# flow exporter exporter-1
switch(config-flow-exporter)# dscp 34
switch(config-flow-exporter)# destination 192.0.2.1 vrf VRF1
switch(config-flow-exporter)# template data timeout 1200
switch(config-flow-exporter)# description Exports flows to 192.0.2.1
```

The following example sets a Traffic Insight instance as the destination for a flow exporter

```
switch(config)# flow exporter exporter-3
switch(config-flow-exporter)# destination type traffic-insight
switch(config-flow-exporter)# destination traffic-insight instance-1
```

The following example adds a destination of each possible type and set **hostname-or-ip-addr** as the type to use:

```
switch(config)# flow exporter exporter-4
switch(config-flow-exporter)# destination collector-1
switch(config-flow-exporter)# destination traffic-insight instance-1
switch(config-flow-exporter)# destination type hostname-or-ip-addr
```

The following example sets an IPv4 address as the destination for a flow exporter

```
switch(config)# flow exporter exporter-1
switch(config-flow-exporter)# destination type hostname-or-ip-addr
switch(config-flow-exporter)# destination 192.168.0.1
```

The following example sets a hostname as the destination for a flow exporter

```
switch(config)# flow exporter exporter-1
switch(config-flow-exporter)# destination type hostname-or-ip-addr
switch(config-flow-exporter)# destination collector1
```

The following example sets an IPv4 address as the destination for a flow exporter with the VRF to which the IPv4 address belongs

```
switch(config)# flow exporter exporter-2
switch(config-flow-exporter)# destination type hostname-or-ip-addr
switch(config-flow-exporter)# destination 192.0.2.1 vrf VRF1
```

The following example sets a Traffic Insight instance as the destination for a flow exporter

```
switch(config)# flow exporter exporter-3
switch(config-flow-exporter)# destination type traffic-insight
switch(config-flow-exporter)# destination traffic-insight instance-1
```

The following example adds a destination of each possible type and set **hostname-or-ip-addr** as the type to use

```
switch(config)# flow exporter exporter-4
```



```
switch(config-flow-exporter)# destination collector-1
switch(config-flow-exporter)# destination traffic-insight instance-1
switch(config-flow-exporter)# destination type hostname-or-ip-addr
```

The following example removes the destination of type **traffic-insight** from a flow exporter:

```
switch(config)# flow exporter exporter-3
switch(config-flow-exporter)# no destination traffic-insight
```

The following example removes the destination of type **hostname-or-ip-addr** from a flow exporter

```
switch(config)# flow exporter exporter-1
switch(config-flow-exporter)# no destination
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification                                             |
|---------|----------------------------------------------------------|
| 10.15   | Command introduced on 9300, 9300S and 6200 Switch series |

## Command Information

| Platforms     | Command context                | Authority                                                                          |
|---------------|--------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>config-flow-exporter | Administrators or local user group members with execution rights for this command. |

## flow monitor

```
flow monitor <name>
 exporter <name>
 cache timeout {inactive <timeout> ||active <timeout>}
 description <description>
```

## Description



If no software augmentation of flows is required, there is no need to configure a flow collector or flow monitor.

| Parameter            | Description                                                     |
|----------------------|-----------------------------------------------------------------|
| <name>               | Name of the flow monitor, up to 64 characters.                  |
| cache timeout active | Use the cache timeout parameter to define an active or inactive |

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | timeout for the flow monitor. A flow monitor closes a flow session that is active for longer than the active timeout or inactive for longer than the inactive timeout.<br>The active timeout range is 30-604800. The default active time out value is 1800 and inactive timeout value is 30.                                                                                                                      |
| cache timeout   | Use the cache timeout parameter to define an inactive timeout for the flow monitor. A flow monitor closes a flow session that is active for longer than the active timeout or inactive for longer than the inactive timeout.<br>For 5420, 6200, 6300, 6400, 8100, 8360, 9300S Switch Series, the inactive timeout range is 30-604800. The default active time out value is 1800 and inactive timeout value is 30. |
| description     | A description up to 256 characters long, including spaces.                                                                                                                                                                                                                                                                                                                                                        |
| exporter <name> | Assign a flow exporter to a flow monitor.                                                                                                                                                                                                                                                                                                                                                                         |
| record <name>   | (For HPE Aruba Networking 5420, 6200, 6300, 6400, 8100, 8325, 8325P, 8325H, 8360, 9300, 9300S Switch series) Assigns a flow record to a flow monitor.                                                                                                                                                                                                                                                             |

## Examples

Create more than the maximum number of allowed flow monitors

```
switch(config)# flow monitor monitor-1
switch(config)# flow monitor monitor-2
No more than 1 flow monitor can be configured. Another flow monitor
must be removed first.
```

Add or modify the description of flow record **\*\*flow-record-1\*\***

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# description Used for basic traffic analysis
```

Add or modify the description of flow exporter **\*\*flow-exporter-1\*\***

```
switch(config)# flow exporter flow-exporter-1
switch(config-flow-exporter)# description Exports flows to 10.2.3.45:2055
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification                                       |
|---------|----------------------------------------------------|
| 10.15   | Command introduced on 9300S and 6200 Switch series |

## Command Information

| Platforms | Command context               | Authority                                                                          |
|-----------|-------------------------------|------------------------------------------------------------------------------------|
| 9300S     | config<br>config-flow-monitor | Administrators or local user group members with execution rights for this command. |

## flow record

```
flow record <record-name>
 match
 ip {source|destination} address
 ip protocol|version
 transport {source | destination} port
 collect
 forwarding-status
 drop ingress-exceptions
 egress interface
 egress queue
 counter {packets|bytes}
 ingress interface
 datalink mac {source | destination} address in
 transport {source | destination} port
 timestamp absolute first
 timestamp absolute last
 description <description>
```

### Description

Creates or modifies a flow record and switches to the **config-flow-record** context for the flow record. Define data to be included in a flow record by configuring flow record match and collect fields.

A flow record defines match (key) fields and collection (non-key) fields. Customers configure flow records with **match** (key) fields and **collect** (non-key) fields. Match fields are the set of fields that define a flow, such as IP address or UDP port. Collect fields are the set of fields that identify information to collect for a flow, such as packet and byte counters.

Traffic with matching attributes (for example, traffic coming from the same interface, sent to the same destination with the same protocol) are classified as a single flow. Information for some or all of the matched settings can be collected and exported to a destination defined by the flow exporter assigned to the flow monitor.



Traffic must match a match rule definition before it can be collected and sent. You cannot collect and send data that is not matched.



A maximum of one flow record can be created for 5420, 8325, 8325H, 8325P, 930 and 9300S Switch series. For 6200, 8360, 8100, 6300, and 6400 Switch series, a maximum of 16 flow records can be created.

| Parameter     | Description                                                             |
|---------------|-------------------------------------------------------------------------|
| <record-name> | Name of the flow monitor, up to 64 characters.                          |
| match         | match traffic according to one or more of the following key attributes: |

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <ul style="list-style-type: none"> <li>▪ <b>ip source:</b> Match traffic from the same IPv4 source.</li> <li>▪ <b>ip destination:</b> Match traffic to the same IPv4 destination.</li> <li>▪ <b>ip protocol:</b> Match traffic using the same IP version</li> <li>▪ <b>ip version:</b> Match traffic using the same IP protocol</li> <li>▪ <b>transport {source   destination} port:</b> Match traffic by source or destination transport port</li> </ul> <p><b>NOTE:</b> The HPE Aruba Networking 8325, 8325H, 8325P and 9300 Switch series support source, destination, and protocol matching on IPv4 networks only.</p>                                                                                                                                                                                                                                                                                                                           |
| description | A description for the flow record up to 256 characters long, including spaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| collect     | <p>Configures data fields to be included a flow record.</p> <ul style="list-style-type: none"> <li>▪ <b>counter bytes:</b> Collect counter data for bytes in the flow. Byte count represents the number of incoming bytes since the previous report.</li> <li>▪ <b>counter packets:</b> Collect counter data for packets in the flow. Packet count represents the number of incoming packets since the previous report.</li> <li>▪ <b>egress interface:</b> Specifies an egress interface as a non-key field in a flow record.</li> <li>▪ <b>egress queue:</b> Specifies an egress queue as a non-key field in a flow record.</li> <li>▪ <b>fowarding status:</b> Specifies forwarding status as a non-key field in a flow record</li> <li>▪ <b>timestamp absolute first:</b> Collect absolute timestamp of the first packet observed.</li> <li>▪ <b>timestamp absolute last:</b> Collect absolute timestamp of the last packet observed.</li> </ul> |

## Examples

Adding timestamp collect fields to **flow-record-1**:

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# collect timestamp absolute last
```

Creating more than the maximum number of allowed flow records:

```
switch(config)# flow record record-1
switch(config)# flow record record-2
No more than 1 flow record can be configured. Another flow record
must be removed first.
```

Adding IPv4 match fields to flow record **flow-record-1** using the **ip** keyword:

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# match ip source address
switch(config-flow-record)# match ip destination address
switch(config-flow-record)# match ip protocol
switch(config-flow-record)# match ip version
```

Removing the IPv4 destination address match field from flow record **flow-record-1** using the **ip** keyword:

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# no match ip destination address
```

Removing the IPv4 destination address match field from flow record **flow-record-1** using the **ipv4** keyword:

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# no match ipv4 destination address
```

Removing the transport destination port match field from flow record **flow-record-1**:

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# no match transport destination port
```

```
switch(config)# flow record flow-record-1
switch(config-flow-record)# collect egress queue threshold
```



To export queue threshold attribute, capture-flows threshold profile should be configured on the egress interfaces. If threshold profile is not configured, congested flows can't be detected and the IEs values are exported as 0. If threshold profile is configured, but collect field is not configured, these IEs are not exported. So in either case, congested flows are not known. For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification                                                                                                                                                                                                                                |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.17   | The <b>collect drop ingress-exceptions</b> parameter is introduced on 5420, 6200, 6200, 8325H, 9300 and 10000 Switch series. Support for <b>egress vlan</b> and <b>egress interface</b> parameters is added on 8100 and 8360 Switch series. |
| 10.16   | Command introduced on 8325P and 9300 Switch series.                                                                                                                                                                                         |
| 10.15   | Command introduced on 6200 and 9300S Switch series                                                                                                                                                                                          |

## Command Information

| Platforms     | Command context              | Authority                                                                          |
|---------------|------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>config-flow-record | Administrators or local user group members with execution rights for this command. |

## ip| flow monitor (interface)

[no] ip| flow monitor (interface)

### Description

Enable flow monitoring on inbound and outbound interfaces by assigning a flow monitor to that interface. Only physical interfaces and LAG interfaces can be monitored. A flow monitor cannot be applied to an interface that is part of a LAG. If an unsupported application is attempted, an error message will be displayed. If the flow monitor is associated with a flow record that contains application fields as collect fields, then Application Recognition should be enabled on the same interface. The **[no]** form of command disables the flow monitoring.



---

An IPv6 flow monitor is not supported on 8325, 8325H, 8325P, and 9300S Switch Series.

---

## Examples

Enable a flow monitor configuration named **flow-monitor-1** for IPv4 traffic on a physical interface.

```
switch(config)# interface 1/1/1
switch(config-if)# ip flow monitor flow-monitor-1 in
```

Associate a flow monitor configuration named **flow-monitor-2** for IPv4 traffic on a LAG interface.

```
switch(config)# interface lag 1
switch(config-if)# ip flow monitor flow-monitor-2 in
```



---

For more information on features that use this command, refer to the Monitoring Guide for your switch model.

---

## Command History

| Release | Modification                                       |
|---------|----------------------------------------------------|
| 10.15   | Command introduced on 9300S and 6200 Switch Series |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>config-flow-monitor | Administrators or local user group members with execution rights for this command. |

## show flow monitor

```
show flow monitor [statistics]
show flow monitor <MONITOR-NAME>[statistics]
```

## Description

Displays flow monitor configuration and status. When no monitor name is specified, the output of this command displays information for all flow monitors.

| Parameter  | Description                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <name>     | Name of the flow monitor.                                                                                                                                                       |
| statistics | For 5420, 6200, 6300, 6400, 8100, 8325, 8325P, 8325H, 8360, 9300, 9300S Switch series, include the <b>statistics</b> parameter to display additional flow and cache statistics. |

## Usage

The output of this command can indicate the following status types:

- Possible status types for all switches
  - Accepted
  - Rejected (Internal error: monitor does not exist)
  - Rejected (The state of one or more of the assigned flow exporters is rejected)
- Possible Status types for 5420 ,6200, 6300, 6400, 8100, 8325 ,8325P, 8325H, 8360, 9300, 9300S Switch series:
  - Rejected (A record must be assigned to the monitor, but no record is assigned)
  - Rejected (The state of the assigned record is rejected)
  - Rejected (Internal error: failure in processing the record configuration)

The possible statistics for a flow monitor are:

| Statistics name        | Meaning                                                                                                                                                         | Switches that support this statistic |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| Current Entries        | Current number of flows in the flow cache for this flow monitor                                                                                                 | 9300<br>9300S                        |
| Flows Added            | Total number of flows added to the flow cache for this flow monitor since it was created                                                                        | 9300<br>9300S                        |
| Total Flows Terminated | Total number of flows removed from the flow cache for this flow monitor since it was created due to any flow end reason                                         | 9300<br>9300S                        |
| Flows Aged             | Number of flows removed from the flow cache for this flow monitor since it was created due to active or inactive timeout                                        | 9300<br>9300S                        |
| Inactive Timeout       | Number of flows removed from the flow cache for this flow monitor since it was created due to inactive cache timeout.                                           | 9300<br>9300S                        |
| Forced End             | Number of flows removed from the flow cache for this flow monitor since it was created due to some external event. For example, the shutdown of a flow monitor. | 9300S                                |

## Examples

Display information for a flow monitor on a 5420, 9300, 9300S Switch series:

```
switch# show flow monitor monitor-1

Flow monitor 'monitor-1'

Description : Used for IPv4 traffic analysis
Status : Accepted
Flow Record : record-1
Flow Exporter(s) : exporter-1
Cache Configuration
Inactive Timeout : 1800
Active Timeout : 300
```

Display information and statistics for a flow monitor on a 9300S Switch series

```
show flow monitor monitor-1 statistics

Flow monitor 'monitor-1'

Current Entries : 2
Flows Added : 6
Total Flows Terminated : 4
 Flows Aged : 2
 Active Timeout :
 Inactive Timeout : 1
 Forced End :
```

Display information and statistics for a flow monitors on a 9300 Switch series:

```
switch# show flow monitor monitor-1 statistics

Flow monitor 'monitor-1'

Current Entries : 2
Flows Added : 6
Total Flows Terminated : 4
Flows Aged : 4
Inactive Timeout : 4
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification                                       |
|---------|----------------------------------------------------|
| 10.15   | Command introduced on 9300S and 6200 Switch series |

## Command Information



| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>config-flow-monitor | Administrators or local user group members with execution rights for this command. |

## show flow record

```
show flow record [<name>]
```

### Description

Display flow record configuration and status. When no record name is specified, the output of this command displays information for all flow records.

The output of this command can indicate the following status types:

- Accepted
- Rejected (Internal error: failed to process record)
- Rejected (Mix of IPv4 and IPv6 match fields is not allowed. Specify match fields of the same IP version (IPv4 or IPv6))

| Parameter | Description              |
|-----------|--------------------------|
| <name>    | Name of the flow record. |

### Examples



IPv6 related commands are only applicable to switches that support IPv6 protocol.

Display the configuration of a flow record named **flow-record-1**.

```
switch# show flow record record-1

Flow record 'record-1'

Description : Used for IPv4 traffic analysis
Status : Accepted
Match Fields
 ipv4 destination address
 ipv4 protocol
 ipv4 source address
 transport destination port
 transport source port
Collect Fields
 counter bytes
 counter packets

 drop ingress-exceptions
```

Display the information of a specific flow record.

```

switch# show flow record record-1

Flow record 'record-1'

Description : Used for IPv4 traffic analysis
Status : Accepted
Match Fields
 ipv4 destination address
 ipv4 protocol
 ipv4 source address

 transport destination port
 transport source port
Collect Fields
 counter bytes
 counter packets

```

### Display information for all flow records

```

switch# show flow record

Flow record 'record-1'

Description : Used for IPv4 traffic analysis
Status : Accepted
Match Fields
 ipv4 destination address
 ipv4 protocol
 ipv4 source address
 transport destination port
 transport source port
Collect Fields
 counter bytes
 counter packets

Flow record 'record-2'

Description : Used for IPv6 traffic analysis
Status : Accepted
Match Fields
 ipv6 destination address
 ipv6 protocol
 ipv6 source address
 ipv6 version
 transport destination port
 transport source port
Collect Fields
 application name
 counter bytes
 counter packets
...

```

### Display information for a specific flow record

```

switch# show flow record record-3

Flow record 'record-3'

Description : Used for IPv4 traffic analysis

```

```
Status : Rejected (Incomplete match fields. The mandatory match
fields are: version, source address,
destination address, protocol, transport destination port, and transport source
port.)
Match Fields
ipv4 destination address
ipv4 protocol
ipv4 source address
ipv4 version
Collect Fields
counter bytes
counter packets
```

Display information with no flow records configured

```
switch# show flow record
No flow records configured
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification                                                                                                                             |
|---------|------------------------------------------------------------------------------------------------------------------------------------------|
| 10.17   | The output of this command includes <b>drop ingress-exceptions</b> information for 5420, 6200, 6200 8325H, 9300 and 10000 Switch series. |
| 10.15   | Command introduced on 6200 and 9300S Switch series                                                                                       |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show tech ipfix

```
show tech ipfix
```

### Description

Shows the IPFIX configuration settings.

If applicable source IP address or source interface is configured for the IPFIX protocol, that configuration is used.

For 6200, 6300, 6400, 8360, 8100 and 9300S Switch Series, If a valid source is configured, the exporter sends flows to an external collector using the effective configured source IP address as the source IP address of the flow packets. In the context of this application, a valid source IP address is any IP address configured in the exporter's VRF namespace.

## Examples

The example shows the IPFIX configuration settings.

```
switch#show tech ipfix
=====
Show Tech executed on Tue Apr 11 02:43:06 2023
=====

[Begin] Feature ipfix
=====

Command : show flow exporter

Flow exporter 'ipfix'

Status : Accepted
Export Protocol : ipfix
Destination Type : Traffic Insight
Destination : t1
Transport Configuration
Protocol : udp
Port : 4739

Flow exporter 'V6E1'

....

[End] Feature ipfix
=====
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification                                        |
|---------|-----------------------------------------------------|
| 10.15   | Command introduced. on 9300S and 6200 Switch Series |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300S     | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## gNMI commands

### crypto pki application gnmi certificate

crypto pki application gnmi certificate <CERT-NAME>

#### Description

Configures a certificate for the gNMI server. **local-cert** is used by default. For more details, refer to the [Public Key Infrastructure guide] (./Functionality\_Guide\_PKI.md)

| Parameter                      | Description                     |
|--------------------------------|---------------------------------|
| <code>&lt;CERT-NAME&gt;</code> | Specifies the certificate name. |

## Examples

Configure sign-cert for the gNMI server:

```
switch(config)# crypto pki application gnmi certificate sign-cert
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config          | Administrators or local user group members with execution rights for this command. |

## gnmi vrf

```
gnmi vrf <VRF NAME>
no gnmi vrf <VRF NAME>
```

## Description

Enables the gNMI server on a given VRF. gNMI can be enabled on multiple VRFs simultaneously.



There is a maximum of 30 gNMI subscriptions per request and a maximum of 9 concurrent streams per switch. These are system-wide limits shared among all authenticated users regardless of connection method (local or remote).

The **no** form of this command removes the configuration.

Disabling the gNMI server on a VRF immediately closes any active streams.

| Parameter                     | Description             |
|-------------------------------|-------------------------|
| <code>&lt;VRF NAME&gt;</code> | Specifies the VRF name. |

## Examples

Enable the gNMI server on VRF mgmt, this allows access to the gNMI server from the OOBM port in the "management VRF":

```
switch(config)# gnmi vrf mgmt
```

Removing the configuration of gNMI server on mgmt:

```
switch(config)# no gnmi vrf mgmt
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config          | Administrators or local user group members with execution rights for this command. |

## show gnmi

show gnmi

### Description

Displays the current gNMI configuration.

### Examples

Display the current gNMI configuration:

```
switch(config)# show gmni
gNMI Configuration

VRF : mgmt, default
Access mode : read-only
Global stream limit : 9
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.17   | Command introduced |

## Command Information

| Platforms | Command context | Authority                                                                                                                                                              |
|-----------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300      | config          | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# Hibernation commands

## hibernate now

hibernate now <END-TIME>

### Description

Activates the switch hibernation immediately. There is no network traffic or activity check on the switch. This command is only available on the VSF conductor and the command execution on the VSF conductor dictates the immediate hibernation of the entire stack.

| Profile names | Description                                               |
|---------------|-----------------------------------------------------------|
| <END_TIME>    | Specifies the hibernation end-time in MM:DD:hh:mm format. |

### Usage

If the same switch configurations are expected to be persistent after the wake-up from hibernation, manually save the current running configurations to the start-up configurations before entering the **hibernation now** command.

Hibernation end-time is a required prerequisite to configure immediate hibernation. The switch cannot enter hibernation if an end-time has not been configured. The end-time must be at least five minutes after the current system time to allow for the system to shutdown safely. It is recommended that the end-time is always greater than the total time taken for the system shutdown.

If the system end-time does not exist or is an incomplete format, an error message is displayed on the console and hibernation does not take place.

### Examples

Enter immediate hibernation and wake up on 10th September at 8:30 PM.

```
switch(config)# hibernate now 09:10:20:30
Checking if the configuration needs to be saved...

Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.
This command will hibernate the system now and wake up at 2025-09-10 20:30.
During that time, the system will not respond to any network traffic and the
console will be inaccessible. The only way to wake up the switch before the
```

hibernation period expires will be to press the mode button on the front panel or to power cycle the switch.

Hibernation fails due to syntax error.

```
switch(config)# hibernate now 09:10:20
The specified hibernation end-time is invalid. This command requires the
hibernation end-time in MM:DD:hh:mm format.
```

Hibernation fails because the end-time is less than five minutes from the current system time.

```
switch(config)# show clock
Tue Feb 28 11:59:00 UTC 2025
System is configured for timezone : UTC
switch(config)# hibernate now 02:28:00:00
The specified hibernation end-time needs to be more than 5 minutes from the
current time.
```

Hibernation fails because the end-time is more than 365 days from the current system time.

```
switch(config)# show clock
Tue Mar 1 00:00:00 UTC 2025
System is configured for timezone : UTC
switch(config)# hibernate now 03:01:00:00
The specified hibernation end-time needs to be at most 365 days from the current
time.
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300S     | config          | Administrators or local user group members with execution rights for this command. |

## hibernate periodic

```
hibernate periodic <RECURRING-DAYS> <START_TIME-END_TIME>
no hibernate periodic <RECURRING-DAYS> <START_TIME-END_TIME>
```

## Description



Enables recurring hibernation mode and configures recurring hibernation options, but it does not hibernate the switch immediately. The configurations are saved as part of the running configuration. To enable recurring hibernation on every hibernation cycle, manually save the configurations. This command is only available on the VSF conductor and the configurations on VSF conductor are retrieved by the entire stack when hibernation mode is triggered.

The **no** form of this command disables recurring hibernation.

| Profile names                            | Description                                                                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;RECURRING_DAYS&gt;</code>      | Specify the recurrence of hibernation. The options are daily, sunday, monday, tuesday, wednesday, thursday, friday, saturday, weekdays, and weekend. |
| <code>&lt;START_TIME-END_TIME&gt;</code> | Specify the hibernation start-time and end-time in "HH:MM-HH:MM" format, up to 10 entries.                                                           |

## Usage

This command allows recurring days to be set as daily, weekdays only, weekend only, or each individual day of the week. It is possible to have seven different profiles catered for each individual day of the week or different profiles for weekdays versus weekend according to business requirements. Each individual day of the week may have up to 10 sets of hibernation configuration timings.

This command enforces the following rules for input parameters:

The end time must always be at least 5 minutes from the start time.

Overlapping time periods are allowed.

To configure for continuous days of hibernation, the user must always ensure that the end time of the last hibernation configuration of a previous day is less than 5 minutes from the start time of the first hibernation configuration of a following day.

If one or more the specified parameters is invalid, an error message is displayed on the console and recurring hibernation configurations is not saved.

The **no** form of this command without the extra parameter disables recurring hibernation. The extra parameter allows the user to disable recurring hibernation and clear configs on a specific day of the week or weekdays or weekend only. There is no need for a reboot for the recurring hibernation disablement to take effect. Manually save the current running configurations to the start-up configurations for them to take affect on the next reboot.

## Examples

Enable recurring hibernation mode.

```
switch(config)# hibernate periodic
This command will enable recurring hibernation mode and hibernate the system
according to the configured recurring hibernation start-time and end-time. During
that time, the system will not respond to any network traffic and the console will
be inaccessible. The only way to wake up the switch before the hibernation period
expires will be to press the mode button on the front panel or to power cycle the
switch.

Continue (y/n)?
```

Hibernate every Monday from 12AM to 9PM.

```
switch(config)# hibernate periodic monday
switch(config-hibernate-mon)# time-period 00:00-09:00
```

Hibernate every Monday from 12AM to 9AM, 12PM to 3 PM, and 7PM to 11:59PM.

```
switch(config)# hibernate periodic monday
switch(config-hibernate-mon)# time-period 00:00-09:00
switch(config-hibernate-mon)# time-period 12:00-15:00
switch(config-hibernate-mon)# time-period 19:00-23:59
```

Hibernate the whole weekend and wake up on Monday 9:00 AM.

```
switch(config)# hibernate periodic weekend
switch(config-hibernate-weekend)# time-period 00:00-23:59
switch(config-hibernate-weekend)# no hibernate periodic monday
This command will clear hibernation configurations for monday only.
Continue (y/n)? y
```

Clear all recurring hibernation configurations.

```
switch(config)# no hibernate periodic daily
This command will clear all hibernation configurations.
Continue (y/n)? y
```

Clear hibernation configurations for weekends.

```
switch(config)# no hibernate periodic weekend
This command will clear all hibernation configurations for weekend only.
Continue (y/n)? y
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300S     | config          | Administrators or local user group members with execution rights for this command. |

## show hibernation

```
show hibernation
```

## Description

Displays the current hibernation configuration and the upcoming hibernation schedule on the switch

## Examples

Display the current hibernation configuration. Enter immediate hibernation and wake up on 10th September at 8:30 PM.

```
switch# show hibernation
Recurring hibernation: Disabled
Recurring configurations:
 Monday:
 00:00 to 08:00
 Saturday:
 00:00 to 09:00
 12:00 to 14:00
 18:00 to 23:59
 Sunday:
 00:00 to 09:00
 12:00 to 23:59
Upcoming hibernation time : NONE
Upcoming wake-up time : NONE
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300S     | config          | Administrators or local user group members with execution rights for this command. |

## show running-config (hibernation)

```
show running-config (hibernation)
```

## Description

Displays the current non-default configuration on the switch. Default hibernation configurations are not displayed in the running-config context.

## Examples

Display the current non-default hibernation configurations on the switch.

```
switch# show running-config
```

```

Current configuration:
!
!Version AOS-CX FL.10.16.0000
!export-password: default
hostname switch
hibernate periodic
hibernate periodic monday
 time-period 00:00-08:00
hibernate periodic saturday
 time-period 00:00-09:00
 time-period 12:00-14:00
 time-period 18:00-23:59
hibernate periodic sunday
 time-period 00:00-09:00
 time-period 12:00-23:59
interface 1/1/1
 no shutdown
 no routing
 vlan access 1
interface 1/1/2
 no shutdown
 no routing
 vlan access 1

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300S     | config          | Administrators or local user group members with execution rights for this command. |

# High Availability Commands

## redundancy switchover

redundancy switchover

### Description

Causes the switch to immediately switch over to the Standby Management Module. This command must be executed from the Active Management Module and will fail if the Standby Management Module is in a failed state or not present.

### Examples

This example shows the redundancy switchover command on an active management module with a standby management module that is present.

```
switch#redundancy switchover
This command causes the switch to immediately switchover to the Standby Management
Module.
Do you want to continue [y/n]?
```

This example shows the redundancy switchover command on an active management module with a standby management module that is absent.

```
switch#redundancy switchover
Standby Management Module not found, switchover request ignored.
```

This example shows the redundancy switchover command on a standby management module.

```
switch#redundancy switchover
Redundancy switchover must be performed from the Active Management Module,
switchover request ignored.
```



For more information on features that use this command, refer to the High Availability Guide for your switch model.

Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## bfd enable

bfd enable  
no bfd enable

### Description

Enables BFD support on an HSC.

The **no** form of this command disables BFD support on an HSC.

### Examples

Enabling BFD:

```
switch(config-hsc)# bfd enable
```

Disabling BFD:

```
switch(config-hsc)# no bfd enable
```



---

For more information on features that use this command, refer to the VXLAN Guide for your switch model.

---

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-hsc      | Administrators or local user group members with execution rights for this command. |

## bfd disable

bfd disable

### Description

Disables BFD support on an HSC.

## Examples

Disabling BFD:

```
switch(config-hsc)# bfd disable
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-hsc      | Administrators or local user group members with execution rights for this command. |

# disable

disable

## Description

Disables a hardware switch controller (HSC).

## Examples

Disabling an HSC:

```
switch(config)# hsc
switch(config-hsc)# disable
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-hsc      | Administrators or local user group members with execution rights for this command. |

## enable

enable  
no enable

### Description

Enables a hardware switch controller (HSC).  
The **no** form of this command disables an HSC.

### Examples

Enabling an HSC:

```
switch(config)# hsc
switch(config-hsc)# enable
Trust Anchor (TA) profile configurations are not used for HSC
authentication. Instead HSC will store the CA certificate from the
HSC controller during the first TLS handshake and use it for all
future authentications with HSC servers. This CA certificate will
not be used for any other certificate-based authentication. Do you
want to continue (y/n)? y
```

Disabling an HSC:

```
switch(config)# hsc
switch(config-hsc)# no enable
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-hsc      | Administrators or local user group members with execution rights for this command. |

## hsc

hsc  
no hsc



## Description

Creates a hardware switch controller (HSC) and changes to the **config-hsc** context for it. The switch uses the HSC to communicate with a remote controller (such as VMware NSX) to create an extended a layer 2 VXLAN network.

The HSC runs an open-source OVSDb server. OVSDb is the Open vSwitch Database Management Protocol detailed in RFC 7047. The remote controller connects to the server as an OVSDb client, and is responsible for managing the interaction with the HSC. As a result, the remote controller is known as the HSC manager.

The **no** form of this command removes the HSC controller and deletes all configuration settings.

## Examples

Creating an HSC:

```
switch(config)# hsc
switch(config-hsc)#
```

Deleting an HSC:

```
switch(config)# no hsc
HSC configuration will be removed.
Do you want to continue (y/n)? y
```



---

For more information on features that use this command, refer to the VXLAN Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## manager ip

```
manager ip <IPV4-ADDR>
no manager ip
```

## Description

Configures the IP address of the HSC manager. The switch can connect with one manager.

The **no** form of this command deletes the IP address of the HSC manager.



---

HSC configuration can only be modified when the HSC is disabled.

---

| Parameter                      | Description                                                                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;IPv4-ADDR&gt;</code> | Specifies the IP address of the HSC manager in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. The IP address must be reachable on the management VRF. |

## Examples

Configuring the IP address of the HSC manager:

```
switch(config)# hsc
switch(config-hsc)# manager ip 1.1.1.1
```

Deleting the HSC manager IP address:

```
switch(config)# hsc
switch(config-hsc)# disable
switch(config-hsc)# no manager ip
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-hsc      | Administrators or local user group members with execution rights for this command. |

## manager port

```
manager port <PORT-NUM>
no manager port
```

### Description

Configures the TCP port on which the HSC communicates with the HSC manager.

The **no** form of this command sets the management port to the default value (6640).



HSC configuration can only be modified when the HSC is disabled.

| Parameter                     | Description                                           |
|-------------------------------|-------------------------------------------------------|
| <code>&lt;PORT-NUM&gt;</code> | TCP port number. Range: 1024 to 65535. Default: 6640. |

## Examples

Configuring port **1055** as the manager port:

```
switch(config)# hsc
switch(config-hsc)# manager port 1055
```

Setting the manager port to the default value:

```
switch(config)# hsc
switch(config-hsc)# disable
switch(config-hsc)# no manager port
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-hsc      | Administrators or local user group members with execution rights for this command. |

### https-server authentication certificate

```
https-server authentication certificate [authorization radius] [username {<CERT-FIELD>}]
```

#### Description

Enables authentication using an x509 certificate for authentication. When this option is configured, the https-server uses the user specified certificate for authentication, and the specified authorization mechanism is used to obtain the corresponding user role. The username embedded in the certificate is used for authorization with a remote user database.

Enabling password authentication is the only way of disabling certificate authentication.



Only one authentication method can be enabled at a time. If you want to disable certificate-based authentication, then the password-based authentication must be enabled.

| Parameter                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;AUTHORIZATION-RADIUS&gt;</code> | <p>Specifies that after certificate authentication succeeds, instead of prompting for a password, the HTTPS server checks the RADIUS server only for authorization.</p> <p>When this parameter is omitted, <b>authorization radius</b> is still the assumed active setting.</p>                                                                                                                               |
| <code>&lt;CERT-FIELD&gt;</code>           | <p>Selects which certificate username field is to be used for authorization.</p> <ul style="list-style-type: none"><li>Specify <b>user_principal_name</b> to use the certificate UserPrincipalName (UPN) field. This is the default.</li><li>Specify <b>common_name</b> to use the certificate CommonName (CN) field.</li></ul> <p>When this parameter is omitted, <b>user_principal_name</b> is assumed.</p> |

#### Example

Enabling authentication using the certificate:

```
switch(config)# https-server authentication certificate authorization radius
username common_name
```

#### Command History

| Release | Modification        |
|---------|---------------------|
| 10.11   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# https-server authentication password

https-server authentication password

## Description

Enables authentication using username and password, which corresponds to the default authentication mechanism. Enabling the password authentication mode disables the certificate authentication mode.



Only one authentication method can be enabled at a time.

## Example

Enabling authentication using the password:

```
switch(config)# https-server authentication password
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.11   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# https-server max-user-sessions

https-server max-user-sessions <SESSION-AMT>

## Description

Sets the maximum amount of concurrent open sessions for any given user through the HTTPS server. The amount of concurrent open sessions may have an impact on system performance, so it is recommended to set this value to the minimum necessary.

| Parameter     | Description                                                                          |
|---------------|--------------------------------------------------------------------------------------|
| <SESSION-AMT> | Specifies the maximum number of user sessions allowed. Default: 6. Maximum value: 8. |

## Example

Set the maximum number of concurrent user sessions to the maximum of 8:

```
switch(config)# https-server max-user-sessions 8
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# https-server rest access-mode

```
https-server rest access-mode {read-only | read-write}
```

## Description

Changes the REST API access mode. The default mode is read-write. This command does not affect Central connections, which have permission to alter configurations regardless of the access mode set on the switch.

| Parameter  | Description                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| read-write | Selects the read/write mode. Allows POST, PUT, PATCH, and DELETE methods to be called on all configurable elements in the switch database. |
| read-only  | Selects the read-only mode. Write access to most switch resources through the REST API is disabled.                                        |

## Usage

Setting the mode to `read-write` on the REST API allows POST, PUT, PATCH, and DELETE methods to be called on all configurable elements in the switch database.

By default, REST APIs in the device are in the read-write mode. Some switch resources allow POST, PUT, PATCH, and DELETE regardless of REST API mode. REST APIs that are required to support the Web UI or the Network Analytics Engine expose POST, PUT, PATCH, or DELETE operations, even if the REST API access mode is set to read-only.

The REST API in read/write mode is intended for use by advanced programmers who have a good understanding of the system schema and data relationships in the switch database.



Because the REST API in read/write mode can access every configurable element in the database, it is powerful but must be used with extreme caution: No semantic validation is performed on the data you write to the database, and configuration errors can destabilize the switch.

## Example

```
switch(config) # https-server rest access-mode read-only
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# https-server rest firmware-site-distribution

```
https-server rest firmware-site-distribution
no https-server rest firmware-site-distribution
```

## Description

This command enables or disables the Firmware Site Distribution server listening on port 9443.

The firmware site distribution allows you to use a switch to distribute a firmware image file to other switches in the same network. This prevents the switches from connecting to the cloud or an external network to download a firmware image file.

On enabling the firmware site distribution, it exposes a REST endpoint that allows the switches to download a switch primary or secondary firmware image.



As per the limitation, up to two switches can download the firmware image simultaneously.

This endpoint is to be used along with REST `/firmware` endpoint to handle the firmware download and installation process.

The **no** form of this command disables the firmware site distribution server.

## Examples

Enabling the HTTPS server firmware site distribution:

```
switch(config)# https-server rest firmware-site-distribution
```

Disabling the HTTPS server firmware site distribution:

```
switch(config)# no https-server rest firmware-site-distribution
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

Executing the HTTPS server firmware site distribution:

```
switch(config)# firmware-site-distribution image <primary|secondary> from
<location> vrf <vrf_name>
```

Here, **location** is the URL source from where the image is going to be downloaded. In FWSD, it's the URL for the seed device with the specified image file (the whole URL path). **primary|secondary** stands for the physical location where the firmware file is going to be downloaded or stored.

## Command History

| Release    | Modification                                                   |
|------------|----------------------------------------------------------------|
| 10.14.1000 | Added command for executing server firmware side distribution. |
| 10.10      | Command introduced.                                            |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# https-server session close all

```
https-server session close all
```

## Description

Invalidates and closes all HTTPS sessions. All existing WebUI sessions (including sessions used for Central connections) will be logged out. REST and WebUI users will have to reauthenticate, and all real-time notification feature WebSocket connections are closed and must be resubscribed.



## Usage

Typically, a user that has consumed the allowed concurrent HTTPS sessions and is unable to access the session cookie to log out manually must wait for the session idle timeout to start another session. This command is intended as a workaround to waiting for the idle timeout to close an HTTPS session. This command stops and starts the `hpe-restd` service, so using this command affects all existing REST sessions, Web UI sessions, and real-time notification subscriptions.

## Example

```
switch# https-server session close all
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# https-server session-timeout

```
https-server session-timeout <MINUTES>
```

## Description

Configures the timeout, in minutes, for any given HTTPS server session. A value of 0 disables the timeout. This command does not affect sessions used for Central connections.

| Parameter | Description                                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MINUTES> | Specifies the maximum idle time, in minutes for an HTTPS session. Default: 20. Maximum: 480 (8 hours). 0 disables the timeout, but the maximum is still enforced. |

## Example

```
switch(config)# https-server session-timeout 10
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## https-server vrf

```
https-server vrf <VRF-NAME>
no https-server vrf <VRF-NAME>
```

### Description

Configures and starts the HTTPS server on the specified VRF, allowing access to REST and the WebUI from ports assigned to that VRF. This command does not affect access to HPE Aruba Networking Central instances, as this feature has its own dedicated connection channel.

The **no** form of the command stops any HTTPS servers running on the specified VRF and removes the HTTPS server configuration.

| Parameter  | Description                                                                  |
|------------|------------------------------------------------------------------------------|
| <VRF-NAME> | Specifies the VRF name. Required. Length: Up to 32 alpha numeric characters. |

### Usage

By using this command, you enable access to both the Web UI and to the REST API on the specified VRF. You can enable access on multiple VRFs.

By default, HPE Aruba Networking 8100, 8320, 8325, 8360, 8400, 9300/9300S, 10000 Switch Series have an HTTPS server enabled on the **mgmt** VRF.

When the HTTPS server is not configured and running, attempts to access the Web UI or REST API result in **404 Not Found** errors.

The VRF you select determines from which network the Web UI and REST API can be accessed.

For example:

- If you want to enable access to the REST API and Web UI through the OOBM port (management IP address), specify the built-in management VRF (**mgmt**).
- If you want to enable access to the REST API and Web UI through the data ports (for "inband management"), specify the built-in default VRF (**default**).

- If you want to enable access to the REST API and Web UI through only a subset of data ports on the switch, specify other VRFs you have created.

HPE Aruba Networking Network Analytics Engine scripts run in the default VRF, but you do not have to enable HTTPS server access on the default VRF for the scripts to run. If the switch has custom HPE Aruba Networking Network Analytics Engine scripts that require access to the Internet, then for those scripts to perform their functions, you must configure a DNS name server on the default VRF.

## Examples

Enabling access on all ports on the switch, specify the default VRF:

```
switch(config)# https-server vrf default
```

Enabling access on the OOBM port (management interface IP address), specify the management VRF:

```
switch(config)# https-server vrf mgmt
```

Enabling access on ports that are members of the VRF named `vrfprogs`, specify `vrfprogs`:

```
switch(config)# https-server vrf vrfprogs
```

Enabling access on the management port and ports that are members of the VRF named `vrfprogs`, enter two commands:

```
switch(config)# https-server vrf mgmt
switch(config)# https-server vrf vrfprogs
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## show https-server

```
show https-server [vsx-peer]
```

## Description

Shows the status and configuration of the HTTPS server. The REST API and web user interface are accessible only on VRFs that have the HTTPS server features configured.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vsx-peer</code> | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Usage

Shows the configuration of the HTTPS server features.

VRF

Shows the VRFs, if any, for which HTTPS server features are configured.

REST Access Mode

Shows the configuration of the REST access mode:

`read-write`

POST, PUT, and DELETE methods can be called on all configurable elements in the switch database. This is the default value.

`read-only`

Write access to most switch resources through the REST API is disabled.

## Examples

```
switch# show https-server

HTTPS Server Configuration

VRF : default, mgmt
REST Access Mode : read-write

Max sessions per user : 6

Session timeout : 20
```



For more information on features that use this command, refer to the Network Analytics Engine Guide or the REST API Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show https-server authentication

show https-server authentication

## Description

Shows the https-server authentication mode status.

## Examples

Showing the authentication method with the password mode enabled:

```
switch# show https-server authentication

Authentication Modes Status

Password Status : enabled

Certificate Status : disabled
```

Showing the authentication method with the certificate mode enabled:

```
switch# show https-server authentication

Authentication Modes Status

Password Status : disabled

Certificate Status : enabled
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.11   | Command Introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show https-serverrest images

show https-server rest images

## Description

Displays the firmware images location for REST usage.

| Parameter | Description                    |
|-----------|--------------------------------|
| images    | Shows firmware image location. |

## Examples

```
switch# show https-server rest images
```

```
REST Software Images Location

primary : "/fwimages/primary.swi"
secondary : "/fwimages/secondary.swi"
```

## Command History

| Release    | Modification        |
|------------|---------------------|
| 10.14.1000 | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## ip icmp redirect

```
ip icmp redirect
no ip icmp redirect
```

### Description

Enables the sending of ICMPv4 and ICMPv6 redirect messages to the source host. Enabled by default. The **no** form of this command disables ICMPv4 and ICMPv6 redirect messages to the source host.

### Examples

Enabling ICMP redirect messages:

```
switch(config)# ip icmp redirect
```

Disabling ICMP redirect messages:

```
switch(config)# no ip icmp redirect
```



---

For more information on features that use this command, refer to the IP Services Guide for your switch model.

---

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip icmp throttle

```
ip icmp throttle <PACKET-INTERVAL>
no ip icmp throttle [<PACKET-INTERVAL>]
```

### Description

Used to configure the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages.

The **no** form of this command disables the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages.

| Parameter                            | Description                                                                            |
|--------------------------------------|----------------------------------------------------------------------------------------|
| <code>&lt;PACKET-INTERVAL&gt;</code> | Specifies the ICMPv4/v6 packet interval in seconds. Default: 1 second. Range: 1-86400. |

## Examples

Enabling the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages:

```
switch(config)# ip icmp throttle 3000
```

Disabling the throttle parameter for both ICMPv4 and ICMPv6 error messages and redirect messages:

```
switch(config)# no ip icmp throttle
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

## Command History

| Release          | Modification                                                                                            |
|------------------|---------------------------------------------------------------------------------------------------------|
| 10.8             | Added the optional <code>&lt;PACKET-INTERVAL&gt;</code> parameter to the <b>no</b> form of the command. |
| 10.07 or earlier | --                                                                                                      |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip icmp unreachable

```
ip icmp unreachable
no ip icmp unreachable
```

### Description

Enables the sending of ICMPv4 and ICMPv6 destination unreachable messages on the switch to a source host when a specific host is unreachable. The unreachable host address originates from the failed packet. Default setting.



The **no** form of this command disables the sending of ICMPv4 and ICMPv6 destination unreachable messages from the switch to a source host when a specific host is unreachable. This command does not prevent other hosts from sending an ICMP unreachable message.

## Examples

Enabling ICMPv4 and ICMPv6 destination unreachable messages to a source host:

```
switch(config)# ip icmp unreachable
```

Disabling ICMPv4 and ICMPv6 destination unreachable messages to a source host:

```
switch(config)# no ip icmp unreachable
```



---

For more information on features that use this command, refer to the IP Services Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

For commands in the interface configuration context, the interface must be an L3 interface. The supported contexts include: `config-if`, `config-if-vlan`, `config-lag-if`, `config-sub-if`.



The sub-interface related configuration examples provided in this section apply only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

## ip igmp

```
ip igmp {enable | disable}
no ip igmp [enable | disable]
```

### Description

Enables or disables IGMP on the current interface. IGMP is disabled by default. The **no** form of this command disables IGMP on the current interface.

| Parameter | Description   |
|-----------|---------------|
| enable    | Enable IGMP.  |
| disable   | Disable IGMP. |

### Examples

Enabling IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp enable
Disabling IGMP on interface VLAN 2:
```

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp disable
```

Enabling IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing

switch(config-subif)# ip igmp enable
```

Disabling IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# ip igmp disable
```

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp enable
```

Enabling IGMP on sub-interface 1/1/1.1:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no shutdown
switch(config-subif)# ip igmp enable
```

Disabling IGMP on sub-interface 1/1/1.1:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# ip igmp disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context                                              | Authority                                                                          |
|--------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if<br>config-subif | Administrators or local user group members with execution rights for this command. |

## ip igmp apply access-list

```
ip igmp apply access-list <ACL-NAME>
no ip igmp apply access-list <ACL-NAME>
```

## Description

Configures the ACL on a particular interface to filter the IGMP join or leave packets based on rules set in the particular ACL name.

The **no** form of this command unconfigures the rules set for the ACL.



This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

| Parameter                     | Description                      |
|-------------------------------|----------------------------------|
| <code>access-list</code>      | Associates an ACL with the IGMP. |
| <code>&lt;ACL-NAME&gt;</code> | Specifies the name of the ACL.   |

## Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

## Examples

Configuring the ACL on a VLAN to filter IGMP packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ip mygroup
switch(config-acl-ip)# 10 deny igmp any 239.255.255.250
switch(config-acl-ip)# 20 deny igmp any 239.255.255.253
switch(config-acl-ip)# 30 permit igmp any 239.1.1.1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-if-vlan)# no ip igmp apply access-list mygroup
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context | Authority                                                                          |
|--------------------------------------------------|-----------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan  | Administrators or local user group members with execution rights for this command. |

## ip igmp last-member-query-interval

```
ip igmp last-member-query-interval <INTERVAL-VALUE>
no ip igmp last-member-query-interval <INTERVAL-VALUE>
```

### Description

Configures an IGMP last member query interval value in seconds on an interface, depending on the command context you are in.

The **no** form of this command sets the value to a default of 1 second on an interface.

| Parameter        | Description                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------|
| <INTERVAL-VALUE> | Specifies an IGMP last-member-query-interval on the interface. Default: 1 second. Range: 1-2 seconds. |

### Examples

Configuring an IGMP last member query interval of 2 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp last-member-query-interval 2
switch(config-if-vlan)# no ip igmp last-member-query-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

# ip igmp querier

```
ip igmp querier
no ip igmp querier
```

## Description

Configures an IGMP querier on an interface, depending on the command context you are in. This functionality will allow an interface to join in the querier-election process.

The **no** form of this command disables IGMP querier on an interface.

## Examples

Configuring an IGMP querier on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier
```

Disabling an IGMP querier on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp querier
```

Configuring an IGMP querier on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp querier
```

Disabling an IGMP querier on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp querier
```

Configuring an IGMP querier on sub-interface 1/1/1.1



---

Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

---

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no shutdown
switch(config-subif)# ip igmp querier
```

Disabling an IGMP querier on sub-interface 1/1/1.1:



---

Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

---

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no ip igmp querier
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                               | Command context                                              | Authority                                                                          |
|-----------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------|
| All , except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if<br>config-subif | Administrators or local user group members with execution rights for this command. |

## ip igmp querier interval

```
ip igmp querier interval <INTERVAL-VALUE>
no ip igmp querier interval
```

### Description

Configures the interval between IGMP queries on an interface, depending on the command context you are in.

The **no** form of this command sets the IGMP querier interval to the default value of 125 seconds on an interface.

| Parameter        | Description                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------|
| <INTERVAL-VALUE> | Specifies the IGMP querier interval in seconds on the interface. Default: 125 seconds. Range: 5-300. |

### Examples

Configuring an IGMP querier interface interval of 100 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier interval 100
```

Resetting an IGMP querier interval to the default value:

```
switch(config-if-vlan)# no ip igmp querier interval
```

Configuring an IGMP querier interface interval of 100 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp querier interval 100
```

Configuring an IGMP querier interface interval of 100 on sub-interface 1/1/1.1:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no shutdown
switch(config-subif)# ip igmp querier interval 100
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context                                              | Authority                                                                          |
|--------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if<br>config-subif | Administrators or local user group members with execution rights for this command. |

## ip igmp querier-wait-time

```
ip igmp querier-wait-time <QUERIER-WAIT-TIME>
no ip igmp querier-wait-time <QUERIER-WAIT-TIME>
```

### Description

Configures initial IGMP querier-wait-time value in seconds.

The **no** form of this command sets the IGMP querier-wait-time to the default value of 260 seconds. Note that the wait timer can be configured to any numbers within the 1-300 second range.

| Parameter           | Description                                         |
|---------------------|-----------------------------------------------------|
| <QUERIER-WAIT-TIME> | Configures IGMP querier-wait-time to desired value. |



## Examples

Configuring IGMP querier-wait-time:

```
switch(config-if-vlan)# ip igmp querier-wait-time
<1-300> Querier Wait value (Default: 260)
switch(config-if-vlan)#
```



When PIM is enabled, automated election will override querier-wait-time configuration. When PIM is disabled and **[no] igmp querier-wait-time** is configured, the initial wait timer will be configured at desired value.

For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.13   | Command introduced. |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

## ip igmp querier query-max-response-time

```
ip igmp querier query-max-response-time <RESPONSE-TIME>
no ip igmp querier query-max-response-time <RESPONSE-TIME>
```

### Description

Configures the IGMP querier max response time value in seconds on an interface, depending on the command context you are in.

The **no** form of this command sets the querier max response time value to the default of 10 seconds on an interface.

| Parameter       | Description                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------|
| <RESPONSE-TIME> | Specifies the IGMP querier max response time value on the interface. Default: 10 seconds. Range: 10-128 seconds. |

## Examples

Configuring the IGMP querier maximum response time of 50 for interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp query-max-response-time 50
```

Resetting an IGMP querier interval to the default value:

```
switch(config-if-vlan)# no ip igmp query-max-response-time
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

## ip igmp robustness

```
ip igmp robustness <VALUE>
no ip igmp robustness <VALUE>
```

### Description

Configures IGMP robustness on an interface, depending on the command context. The robustness parameter allows tuning for the expected packet loss on a subnet.

The **no** form of this command sets the robustness value to the default of 2 on an interface.

| Parameter | Description                                                                  |
|-----------|------------------------------------------------------------------------------|
| <VALUE>   | Specifies an IGMP robustness value on the interface. Default: 2. Range: 1-7. |

### Examples

Configuring an IGMP robustness of 5 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp robustness 5
```

Resetting the IGMP robustness to the default:

```
switch(config-if-vlan)# no ip igmp robustness
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

## ip igmp router-alert-check

```
ip igmp router-alert-check [enable | disable]
no ip igmp router-alert-check [enable | disable]
```

### Description

Enables or disables IGMP router alert check for IGMP packets. IGMP packets without the router alert field set are dropped if router alert check is enabled. Router alert check is disabled by default.

The **no** form of this command disables router alert check for IGMP packets.

| Parameter | Description                      |
|-----------|----------------------------------|
| enable    | Enable IGMP router alert check.  |
| disable   | Disable IGMP router alert check. |

### Examples

Enabling IGMP router alert check on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp router-alert-check enable
```

Disabling IGMP router alert check on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp router-alert-check disable
```

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp router-alert-check enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.08   | Command introduced. |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

## ip igmp static-group

```
ip igmp static-group <MULTICAST-GROUP-IP>
no ip igmp static-group <MULTICAST-GROUP-IP>
```

### Description

Configures an IGMP static multicast group on an interface, depending on the command context you are in. You can configure a maximum of 32 IGMP static groups.

The **no** form of the command unconfigures IGMP static multicast group on an interface.

| Parameter            | Description                                                                           |
|----------------------|---------------------------------------------------------------------------------------|
| <MULTICAST-GROUP-IP> | Specifies an IGMP static multicast group IP address on the interface. Format: A.B.C.D |

### Examples

Administrators or local user group members with execution rights for this command.

Configuring an IGMP static group on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp static-group 239.1.1.1
```

Resetting an IGMP static group on an interface to the default (none):

```
switch(config-if)# no ip igmp static-group 239.1.1.10
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.13   | Command introduced. |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

## ip igmp version

```
ip igmp version <VERSION>
no ip igmp version <VERSION>
```

### Description

Configures the IGMP version on an interface, depending on the command context you are in. The **no** form of the command configures the default IGMP version, 3, on the interface.

| Parameter | Description                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------|
| <VERSION> | Specifies the IGMP version on the interface. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3. |

### Examples

Configuring an IGMP version on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp version 2
```

Configuring an IGMP version on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip igmp version 2
```

Removing an IGMP version on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp version 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

## ip igmp version strict

```
ip igmp version <VERSION> strict
no ip igmp version <VERSION> strict
```

### Description

Configures an IGMP strict version on an interface, depending on the command context you are in. Drops packets that do not match the configured version.

The **no** form of the command removes the strict version configuration from the interface.

| Parameter | Description                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------|
| <VERSION> | Specifies the IGMP version on the interface. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3. |

### Examples

Configuring the IGMP strict version to 2 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp version 2 strict
```

Resetting the IGMP strict version to the default (none):

```
switch(config-if)# no ip igmp version 2 strict
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context                              | Authority                                                                          |
|--------------------------------------------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

# no ip igmp

no ip igmp

## Description

Disables all IGMP configurations on an interface or sub-interface, depending on the command context you are in.

## Examples

Removing IGMP on interface VLAN 2:

```
switch(config) # interface vlan 2
switch(config-if-vlan) # no ip igmp
```

Removing IGMP on interface 1/1/1:

```
switch(config) # interface 1/1/1
switch(config-subif) # no ip igmp
```

Removing IGMP on sub-interface 1/1/1.1:

```
switch(config) # interface 1/1/1.1
switch(config-subif) # no ip igmp
```



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context                                              | Authority                                                                          |
|--------------------------------------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | config-if-vlan<br>config-if<br>config-lag-if<br>config-subif | Administrators or local user group members with execution rights for this command. |

## show ip igmp

```
show ip igmp [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

### Description

Shows IGMP configuration information and status, or shows information by VRF.

| Parameter                 | Description                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf <VRF-NAME>   all-vrfs | Optional. Used to show information by VRF. Specify the VRF by VRF name. With no <VRF-NAME> specified, the default VRF is implied. To show information for all VRFs, specify <b>all-vrfs</b> .                                    |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Showing IGMP configuration and status:

```
switch# show ip igmp

VRF Name : default
Interface : vlan2
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 20.1.1.1
Querier Uptime : 1m 4s
Querier Expiration Time : 0m 1s
IGMP Snoop Enabled on VLAN : True
```



Showing IGMP information for VRF test:

```
switch# show ip igmp vrf test

VRF Name : test
Interface : 1/1/2
IGMP Configured Version : 3
IGMP Operating Version : 2
Querier State : Querier
Querier IP [this switch] : 100.1.1.1
Querier Uptime : 2m 55s
Querier Expiration Time : 0m 16s

Active Group Address Vers Mode Uptime Expires

240.100.3.194 3 INC 0m 30s 3m 50s

IGMP is not enabled on interface 1/1/3

VRF Name : test
Interface : vlan2
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 20.1.1.1
Querier Uptime : 1m 4s
Querier Expiration Time : 0m 1s
IGMP Snoop Enabled on VLAN : True

Active Group Address Vers Mode Uptime Expires

238.224.153.165 2 0m 38s 3m 42s

VRF Name : test
Interface : vlan10
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 10.1.1.1
Querier Uptime : 1m 4s
Querier Expiration Time : 0m 1s
IGMP Snoop Enabled on VLAN : True

Active Group Address Vers Mode Uptime Expires

239.209.3.194 3 INC 0m 38s 3m 42s
```

Showing IGMP information for all VRFs:

```
switch# show ip igmp all-vrfs

VRF Name : test
Interface : 1/1/2
IGMP Configured Version : 3
IGMP Operating Version : 2
Querier State : Querier
Querier IP [this switch] : 100.1.1.1
Querier Uptime : 2m 55s
Querier Expiration Time : 0m 16s
```

```

Active Group Address Vers Mode Uptime Expires

240.100.3.194 3 INC 0m 30s 3m 50s

```

```

VRF Name : test
Interface : vlan2
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 20.1.1.1
Querier Uptime : 1m 4s
Querier Expiration Time : 0m 1s
IGMP Snoop Enabled on VLAN : True

```

```

Active Group Address Vers Mode Uptime Expires

238.224.153.165 2 0m 38s 3m 42s

```

```

VRF Name : default
Interface : vlan5
IGMP Configured Version : 3
IGMP Operating Version : 2
Querier State : Querier
Querier IP [this switch] : 50.1.1.1
Querier Uptime : 1m 1s
Querier Expiration Time : 0m 4s
IGMP Snoop Enabled on VLAN : False

VRF Name : test
Interface : vlan10
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 10.1.1.1
Querier Uptime : 1m 4s
Querier Expiration Time : 0m 1s
IGMP Snoop Enabled on VLAN : True

```

```

Active Group Address Vers Mode Uptime Expires

239.209.3.194 3 INC 0m 38s 3m 42s

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ip igmp counters

show ip igmp counters [vrf <VRF-NAME> | all-vrfs] [vsx-peer]

## Description

Shows IGMP counter details, or shows counters by VRF.

| Parameter                 | Description                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf <VRF-NAME>   all-vrfs | Optional. Used to show information by VRF. Specify the VRF by VRF name. With no <VRF-NAME> specified, the default VRF is implied. Specify <b>all-vrfs</b> to show information for all VRFs.                                      |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP counters:

```
switch# show ip igmp counters

IGMP Counters

Interface Name : vlan2
VRF Name : default
Membership Timeout : 0

 Rx Tx

V1 All Hosts Queries 0 0
V2 All Hosts Queries 0 12
V3 All Hosts Queries 0 0
V2 Group Specific Queries 0 0
V3 Group Specific Queries 0 0
Group And Source Specific Queries 0 0
V3 Member Reports 0 N/A
V2 Member Reports 0 N/A
V1 Member Reports 0 N/A
V2 Member Leaves 0 N/A
Packets dropped by ACL 0 N/A
```

Showing IGMP counters for the default VRF:

```
switch# show ip igmp counters vrf default

IGMP Counters

Interface Name : vlan2
VRF Name : default
Membership Timeout : 0

 Rx Tx

V1 All Hosts Queries 0 0
V2 All Hosts Queries 0 12
```

|                                   |   |     |
|-----------------------------------|---|-----|
| V3 All Hosts Queries              | 0 | 0   |
| V2 Group Specific Queries         | 0 | 0   |
| V3 Group Specific Queries         | 0 | 0   |
| Group And Source Specific Queries | 0 | 0   |
| V3 Member Reports                 | 0 | N/A |
| V2 Member Reports                 | 0 | N/A |
| V1 Member Reports                 | 0 | N/A |
| V2 Member Leaves                  | 0 | N/A |
| Packets dropped by ACL            | 0 | N/A |



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ip igmp group

```
show ip igmp group <GROUP-IP> [source <SOURCE-IP>] [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

## Description

Shows IGMP joined group information for the specified group, or shows joined group source and display information by VRF.

| Parameter                 | Description                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <GROUP-IP>                | Specifies the IP address of the group. Format: A.B.C.D                                                                                                                                                                           |
| source <SOURCE-IP>        | Specifies the IP address of the source. Format: A.B.C.D                                                                                                                                                                          |
| vrf <VRF-NAME>   all-vrfs | Optional. Used to show information by VRF. Specify the VRF by VRF name. With no <VRF-NAME> specified, the default VRF is implied. Specify <b>all-vrfs</b> to show information for all VRFs.                                      |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP joined group details for group 239.1.1.10:

```
switch# show ip igmp group 239.1.1.10

IGMP group information for group 239.1.1.10

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 EXC 16m 34s 2m 27s Timer Timer Forwarded Blocked
```

Showing IGMP joined group details for group 239.1.1.10 and source 10.1.1.10:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10

Interface Name : vlan2
VRF Name : default
Group Address : 239.1.1.10
Source Address : 10.1.1.10

Mode Uptime Expire
----- -
 0m 13s 4m 7s
```

Showing IGMP joined group details for group 239.1.1.10 for all VRFs:

```
switch# show ip igmp group 239.1.1.10 all-vrfs

IGMP group information for group 239.1.1.10

Interface Name : vlan10
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 EXC 17m 5s 4m 2s Timer Timer Forwarded Blocked
```

Showing IGMP joined group details for group 239.1.1.10 source 10.1.1.10 for all VRFs:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10 all-vrfs

Interface Name : vlan10
VRF Name : default
Group Address : 239.1.1.10
Source Address : 10.1.1.10
```

| Mode | Uptime | Expire |
|------|--------|--------|
| ---- | -----  | -----  |
|      | 0m 39s | 3m 41s |

Showing IGMP joined group details group 239.1.1.10 for the default VRF:

```
switch# show ip igmp group 239.1.1.10 vrf default

IGMP group information for group 239.1.1.10

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 EXC 17m 35s 3m 32s Timer Timer Forwarded Blocked
```

Showing IGMP joined group details group 239.1.1.10 source 10.1.1.10 for the default VRF:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10 vrf default

Interface Name : vlan10
VRF Name : default
Group Address : 239.1.1.10
Source Address : 10.1.1.10

Mode Uptime Expire
---- -
0m 59s 3m 21s
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show ip igmp groups

```
show ip igmp groups [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

## Description

Shows IGMP group information, or you can display group information by VRF.

| Parameter                 | Description                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf <VRF-NAME>   all-vrfs | Optional. Used to show information by VRF. Specify the VRF by VRF name. With no <VRF-NAME> specified, the default VRF is implied. Specify <b>all-vrfs</b> to show information for all VRFs.                                      |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP group information:

```
switch# show ip igmp groups

IGMP group information for group 239.1.1.10

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 EXC 0m 36s 3m 44s Timer Timer Forwarded Blocked

IGMP group information for group 239.1.1.11

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.11
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 EXC 0m 36s 3m 44s Timer Timer Forwarded Blocked
```

Showing IGMP groups for all VRFs:

```
switch# show ip igmp groups all-vrfs
IGMP group information for group 239.1.1.1

Interface Name : vlan10
VRF Name : test
```

Group Address : 239.1.1.1  
Last Reporter : 100.1.1.20

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 0m 13s | 4m 7s   |             |             |                      |                    |

IGMP group information for group 239.1.1.2

Interface Name : vlan10  
VRF Name : test

Group Address : 239.1.1.2  
Last Reporter : 100.1.1.20

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 0m 13s | 4m 7s   |             |             |                      |                    |

IGMP group information for group 239.1.1.1

Interface Name : vlan10  
VRF Name : test

Group Address : 239.1.1.1  
Last Reporter : 100.1.1.20

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 0m 13s | 4m 7s   |             |             |                      |                    |

IGMP group information for group 239.1.1.2

Interface Name : vlan10  
VRF Name : test

Group Address : 239.1.1.2  
Last Reporter : 100.1.1.20

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 0m 13s | 4m 7s   |             |             |                      |                    |

IGMP group information for group 239.1.1.1

Interface Name : vlan20  
VRF Name : default

Group Address : 239.1.1.1  
Last Reporter : 200.1.1.10

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 0m 13s | 4m 7s   |             |             |                      |                    |

IGMP group information for group 239.1.1.2



```

Interface Name : vlan20
VRF Name : default

Group Address : 239.1.1.2
Last Reporter : 200.1.1.10

```

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 0m 13s | 4m 7s   |             |             |                      |                    |

Showing IGMP groups for the default VRF:

```
switch# show ip igmp groups vrf default
```

IGMP group information for group 239.1.1.10

```

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

```

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 9m 23s | 3m 20s  |             |             |                      |                    |

IGMP group information for group 239.1.1.11

```

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.11
Last Reporter : 100.1.1.10

```

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 9m 23s | 3m 20s  |             |             |                      |                    |

IGMP group information for group 239.1.1.10

```

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.10
Last Reporter : 100.1.1.10

```

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 9m 23s | 3m 20s  |             |             |                      |                    |

IGMP group information for group 239.1.1.11

```

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.11
Last Reporter : 100.1.1.10

```

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | EXC  | 9m 23s | 3m 20s  |             |             |                      |                    |



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp interface

```
show ip igmp interface [{<INTF-ID>|<INTF-ID.ID>|{vlan <VLAN-ID>}}]
counters [vsx-peer]
group <A.B.C.D> [{source <A.B.C.D>}] [vsx-peer]
groups [vsx-peer]
statistics [vsx-peer]
[vsx-peer]
```

## Description

Shows IGMP configuration information for a specific interface (VLAN, port or LAG).

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTF-ID>      | Specifies an interface (such as 1/1/2 or LAG10).                                                                                                                                                                                 |
| <INTF-ID.ID>   | Required. Specifies a sub-interface. (Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.)                                                                  |
| vlan <VLAN-ID> | Specifies a VLAN. Values: 1-4094.                                                                                                                                                                                                |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP configuration information for interface VLAN 2:

```
switch# show ip igmp interface vlan 2

IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 20.1.1.1
Querier Uptime : 1m 46s
Querier Expiration Time : 0m 1s
Snoop Enabled on VLAN : True

switch# show ip igmp interface vlan 10

IGMP is not enabled
```

Showing IGMP configuration information for the specified interface 1/1/2:

```
switch# show ip igmp interface 1/1/2

IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 100.1.1.1
Querier Uptime : 51m 44s
Querier Expiration Time : 1m 51s
```

Showing IGMP configuration information for sub-interface 1/1/5.10:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch# show ip igmp interface 1/1/5.10

IGMP Configured Version : 3
IGMP Operating Version : 3
Querier State : Querier
Querier IP [this switch] : 200.1.1.1
Querier Uptime : 11m 44s
Querier Expiration Time : 1m 51s
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp interface counters

show ip igmp interface {<INTF-ID> | <INTF-ID.ID>} vlan <VLAN-ID> counters [vsx-peer]

### Description

Shows IGMP counter details for a specific interface or VLAN interface.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTF-ID>      | Specifies an interface (such as 1/1/2).                                                                                                                                                                                          |
| <INTF-ID.ID>   | Required: Specifies a sub-interface. (Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.)                                                                  |
| vlan <VLAN-ID> | Specifies a VLAN. Values: 1-4094.                                                                                                                                                                                                |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Showing IGMP counters for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 counters
```

```
IGMP Counters
```

```
Interface Name : vlan2
VRF Name : default
Membership Timeout : 0
```

|                                   | Rx    | Tx    |
|-----------------------------------|-------|-------|
|                                   | ----- | ----- |
| V1 All Hosts Queries              | 0     | 0     |
| V2 All Hosts Queries              | 0     | 0     |
| V3 All Hosts Queries              | 0     | 29    |
| V2 Group Specific Queries         | 0     | 0     |
| V3 Group Specific Queries         | 0     | 2     |
| Group And Source Specific Queries | 0     | 2     |
| V3 Member Reports                 | 0     | N/A   |
| V2 Member Reports                 | 0     | N/A   |
| V1 Member Reports                 | 0     | N/A   |
| V2 Member Leaves                  | 0     | N/A   |
| Packets dropped by ACL            | 0     | N/A   |

Showing IGMP counters for sub-interface 10:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 counters
```

#### IGMP Counters

Interface Name : 1/1/5.10  
VRF Name : default  
Membership Timeout : 0

|                                   | Rx    | Tx    |
|-----------------------------------|-------|-------|
|                                   | ----- | ----- |
| V1 All Hosts Queries              | 0     | 0     |
| V2 All Hosts Queries              | 0     | 0     |
| V3 All Hosts Queries              | 0     | 9     |
| V2 Group Specific Queries         | 0     | 0     |
| V3 Group Specific Queries         | 0     | 0     |
| Group And Source Specific Queries | 0     | 0     |
| V3 Member Reports                 | 3     | N/A   |
| V2 Member Reports                 | 4     | N/A   |
| V1 Member Reports                 | 0     | N/A   |
| V2 Member Leaves                  | 0     | N/A   |
| Packets dropped by ACL            | 0     | N/A   |



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp interface group

```
show ip igmp [interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} [group <GROUP-IP> [source <SOURCE-IP>] [vsx-peer]]]
```

### Description

Shows IGMP joined group information for a specific interface or VLAN interface, or specify a source IP.

| Parameter          | Description                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTF-ID>          | Specifies an interface (such as 1/1/2).                                                                                                                                                                                          |
| <INTF-ID.ID>       | Required: Specifies the sub-interface. (Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.)                                                                |
| vlan <VLAN-ID>     | Specifies a VLAN. Values: 1-4094.                                                                                                                                                                                                |
| <GROUP-IP>         | Specifies the IP address of the group. Format: A.B.C.D                                                                                                                                                                           |
| source <SOURCE-IP> | Specifies the IP address of the source. Format: A.B.C.D                                                                                                                                                                          |
| vsx-peer           | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP joined group details for group 239.1.1.1 for interface VLAN 10:

```
switch# show ip igmp interface vlan 10 group 239.1.1.1

IGMP group information for group 239.1.1.1

Interface Name : vlan10
VRF Name : default

Group Address : 239.1.1.1
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 INC 8m 10s 2m 21s Timer Timer Forwarded Blocked

Group Address : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime Expire
----- -
INC 8m 10s 2m 21s
```

Showing IGMP joined group details for group 239.1.1.1 for interface VLAN 10 with source details for 10.1.1.1:

```
switch# show ip igmp interface vlan 10 group 239.1.1.1 source 10.1.1.1

Interface Name : vlan10
VRF Name : default
Group Address : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime Expire
----- -
INC 8m 52s 3m 51s
```

Showing IGMP joined group details for group 239.1.1.1 for sub-interface 1/1/1.10:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 group 239.1.1.1

IGMP group information for group 239.1.1.1

Interface Name : 1/1/5.10
VRF Name : default

Group Address : 239.1.1.1
Last Reporter : 10.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 INC 1m 49s 1m 31s Timer Timer Forwarded Blocked
----- -

Group Address : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime Expire
---- -
INC 1m 49s 1m 31s
```

Showing IGMP joined group details for group 239.1.1.1 for sub-interface 1/1/1.10 with source details for 10.1.1.1:

```
switch# show ip igmp interface 1/1/5.10 group 239.1.1.1 source 10.1.1.1

Interface Name : 1/1/5.10
VRF Name : default
Group Address : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime Expire
---- -
INC 1m 3s 4m 25s
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp interface groups

```
show ip igmp [interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} [groups] [vsx-peer]]
```

### Description

Shows IGMP group information for a specific interface or VLAN interface.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTF-ID>      | Specifies an interface (such as 1/1/2).                                                                                                                                                                                          |
| <INTF-ID.ID>   | Required: Specifies the sub-interface. (Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.)                                                                |
| vlan <VLAN-ID> | Specifies a VLAN. Values: 1-4094.                                                                                                                                                                                                |
| <GROUP-IP>     | Specifies the IP address of the group. Format: A.B.C.D                                                                                                                                                                           |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Showing IGMP groups for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 groups

IGMP group information for group 239.1.1.1

Interface Name : vlan2
VRF Name : default

Group Address : 239.1.1.1
Last Reporter : 100.1.1.10

Vers Mode Uptime Expires V1 V2 Sources Sources
----- -
3 INC 4m 40s 3m 51s Timer Timer Forwarded Blocked

Group Address : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime Expire

INC 4m 40s 3m 51s
```



IGMP group information for group 239.1.1.2

Interface Name : vlan2  
VRF Name : default

Group Address : 239.1.1.2  
Last Reporter : 100.1.1.10

| Vers | Mode | Uptime | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|--------|---------|-------------|-------------|----------------------|--------------------|
| 3    | INC  | 4m 40s | 3m 51s  |             |             | 1                    |                    |

Group Address : 239.1.1.2  
Source Address : 10.1.1.1

| Mode | Uptime | Expire |
|------|--------|--------|
| INC  | 4m 40s | 3m 51s |

Showing IGMP groups for sub-interface:

```
switch# show ip igmp interface 1/1/5.10 groups
```

IGMP group information for group 239.1.1.1

Interface Name : 1/1/5.10  
VRF Name : default

Group Address : 239.1.1.10  
Last Reporter : 10.1.1.1

| Vers | Mode | Uptime  | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|---------|---------|-------------|-------------|----------------------|--------------------|
| 2    |      | 11m 59s | 1m 44s  |             | 1m 44s      |                      |                    |

IGMP group information for group 239.1.1.2

Interface Name : 1/1/5.10  
VRF Name : default

Group Address : 239.1.1.20  
Last Reporter : 10.1.1.10

| Vers | Mode | Uptime  | Expires | V1<br>Timer | V2<br>Timer | Sources<br>Forwarded | Sources<br>Blocked |
|------|------|---------|---------|-------------|-------------|----------------------|--------------------|
| 2    |      | 11m 59s | 1m 44s  |             | 1m 44s      |                      |                    |



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp interface statistics

show ip igmp interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} statistics [vsx-peer]

### Description

Shows IGMP statistics for a specific interface or VLAN interface, including groups joined.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTF-ID>      | Specifies an interface (such as 1/1/2 or LAG1).                                                                                                                                                                                  |
| <INTF-ID.ID>   | Required: Specifies the sub-interface. (Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.)                                                                |
| vlan <VLAN-ID> | Specifies a VLAN. Values: 1-4094.                                                                                                                                                                                                |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Showing IGMP statistics for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 statistics

IGMP statistics

Interface Name : vlan2
VRF Name : default

Number of Include Groups : 2
Number of Exclude Groups : 0
Number of Static Groups : 0
Total Multicast Groups Joined : 2
```

Showing IGMP statistics for the sub-interface:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 statistics

IGMP statistics

Interface Name : 1/1/5.10
VRF Name : default

Number of Include Groups : 0
Number of Exclude Groups : 2
Number of Static Groups : 0
Total Multicast Groups Joined : 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.17            | Sub-interface support extended to 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp static-groups

```
show ip igmp static-groups [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

### Description

Shows IGMP static groups, or shows information by VRF.

| Parameter                 | Description                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf <VRF-NAME>   all-vrfs | Optional. Used to show information by VRF. Specify the VRF by VRF name. With no <VRF-NAME> specified, the default VRF is implied. Specify <b>all-vrfs</b> to show information for all VRFs. |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the                                                        |

| Parameter | Description                                                                                 |
|-----------|---------------------------------------------------------------------------------------------|
|           | VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP static-group information:

```
switch# show ip igmp static-groups

IGMP Static Group Address Information

VRF Name default
Interface Name Group Address

vlan10 238.1.1.1
```

Showing IGMP statics-group information for all VRFs:

```
switch# show ip igmp static-groups all-vrfs

IGMP Static Group Address Information
VRF Name :test
Interface Name Group Address

vlan20 239.1.1.1
VRF Name :default
Interface Name Group Address

vlan10 238.1.1.1
```

```
Showing IGMP static-group information for VRF test:
switch# show ip igmp static-groups vrf test

IGMP Static Group Address Information

VRF Name :test
Interface Name Group Address

vlan20 239.1.1.1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip igmp statistics

```
show ip igmp statistics [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

### Description

Shows IGMP statistics, including groups joined, or shows statistics by VRF.

| Parameter                 | Description                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vrf <VRF-NAME>   all-vrfs | Optional. Used to show information by VRF. Specify the VRF by VRF name. With no <VRF-NAME> specified, the default VRF is implied. Specify <b>all-vrfs</b> to show information for all VRFs.                                      |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Showing IGMP statistics:

```
switch# show ip igmp statistics
IGMP statistics

VRF Name : default

Number of Include Groups : 1
Number of Exclude Groups : 0
Number of Static Groups : 0
Total Multicast Groups Joined : 1
```

Showing IGMP statistics for all VRFs:

```
switch# show ip igmp statistics all-vrfs
IGMP statistics
VRF Name : test

Number of Include Groups : 2
Number of Exclude Groups : 0
Number of Static Groups : 0
Total Multicast Groups Joined : 2
VRF Name : default

Number of Include Groups : 1
Number of Exclude Groups : 0
Number of Static Groups : 0
```

```
Total Multicast Groups Joined : 1
```

Showing IGMP statistics for VRF test:

```
switch# show ip igmp statistics vrf test
IGMP statistics

VRF Name : test

Number of Include Groups : 2
Number of Exclude Groups : 0
Number of Static Groups : 0
Total Multicast Groups Joined : 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms                                        | Command context             | Authority                                                                                                                                                              |
|--------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms, except for S3L75A, S3L76A, S3L77A | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## Inband Flow Analyzer (IFA) commands

---

### class

```
class {ifa-ip | ifa-ipv6} <NAME>
no class {ifa-ip | ifa-ipv6} <NAME>
```

#### Description

Creates a new IFA class for IPv4 or IPv6 traffic.

The **no** form of this command removes an IFA class for IPv4 or IPv6 traffic.

| Parameter | Description                                               |
|-----------|-----------------------------------------------------------|
| ifa-ip    | Specifies the IFA based Internet Protocol v4 (IFA-IPv4) . |
| ifa-ipv6  | Specifies the IFA based Internet Protocol v6 (IFA-IPv6) . |
| <NAME>    | Specifies the IFA class name.                             |

#### Examples

Configuring an IFA IPv4 class:

```
switch(config)# class ifa-ip IFA_Class
```

Configuring an IFA IPv6 class:

```
switch(config)# class ifa-ipv6 IFA_IPv6_Class
```

Removing an IFA class for IPv4 or IPv6 traffic:

```
switch(config)# no class ifa-ip IFA_Class
```

```
switch(config)# no class ifa-ipv6 IFA_IPv6_Class
```



---

For more information on features that use this command, refer to the Monitoring Guide for your switch model.

---

#### Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## class ipv4/ipv6 filter

```
[<sequence_number>
 {match|ignore}
 {udp|tcp}
 {any|<src_ip_address>[/<prefix_length>|<subnet_mask>]]}
 [any|{eq|gt|lt} <source_port_number>|range <port_number> <port_number>]
 {any|<dst_ip_address>[/<prefix_length>|<subnet_mask>]]}
 [any|{eq|gt|lt} <destination_port_number>|range <port_number> <port_number>]
no <sequence_number>
```

## Description

Configures an IFA IPv4 or IPv6 Flow Filter Class based on 5-tuple. The IFA Flow Filter can filter by protocols UDP and TCP, source IP, source port, destination IP, and destination port.

The **no** form of this command removes the IFA Flow Filter Class based on the entry sequence number.

| Parameter                            | Description                                                               |
|--------------------------------------|---------------------------------------------------------------------------|
| <code>&lt;sequence_number&gt;</code> | Specifies a sequence number for the match number. Range: 1 to 4294967295. |
| <code>udp</code>                     | Specifies the user datagram protocol.                                     |
| <code>tcp</code>                     | Specifies the transmission datagram protocol.                             |
| <code>&lt;src_ip_address&gt;</code>  | Specifies the source IP host address.                                     |
| <code>&lt;prefix_length&gt;</code>   | Specifies the source or destination prefix length.                        |
| <code>&lt;subnet_mask&gt;</code>     | Specifies the source or destination network mask.                         |
| <code>&lt;dst_ip_address&gt;</code>  | Specifies the destination IP host address.                                |
| <code>any</code>                     | Specifies any source or destination IP address.                           |
| <code>eq</code>                      | Specifies the Layer 4 port.                                               |
| <code>gt</code>                      | Specifies the Layer 4 port greater than the indicated port.               |
| <code>lt</code>                      | Specifies the Layer 4 port lesser than the indicated port.                |



## Examples

Configuring an IFA IPv4 Flow Filter **match** with all the available parameters (5-tuple):

```
switch(config-class-ifa-ip)# 1 match tcp 10.10.10.10 eq 5 1.1.1.1 eq 10
```

Configure an IFA Flow Filter **ignore** with all the available parameters (5-tuple):

```
switch(config-class-ifa-ip)# 1 ignore tcp 10.10.10.10 eq 5 1.1.1.1 eq 10
```

Configuring an IFA IPv6 Flow Filter **match** with all the available parameters (5-tuple):

```
switch(config-class-ifa-ip)# 1 match tcp 10:10::10:10 eq 5 1:1::1:1 eq 10
```

Configuring an IFA IPv6 Flow Filter Match with source and destination IP:

```
switch(config-class-ifa-ip)# 1 match 10:10::10:10 1:1::1:1
```

Removing an IFA Flow Filter Class match:

```
switch(config-class-ifa-ip)# no 1
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-class-ifa-ip | Administrators or local user group members with execution rights for this command. |

## flow-filter-class

```
flow-filter-class <NAME>
no flow-filter-class
```

### Description

Assigns a Flow Filter Class to a specific IFA Initiator Flow Monitor. Each class can classify traffic based on the IPv4 or IPv6 header information, using special IFA IPv4 and IPv6 class types.

The **no** form of this command removes a Flow Filter Class from a specific IFA initiator monitor.

| Parameter | Description                           |
|-----------|---------------------------------------|
| <NAME>    | Specifies the flow filter class name. |

## Examples

Assigning a Flow Filter Class to an IFA Initiator Monitor on the system:

```
switch(config-flow-ifa-initiator-monitor)# flow-filter-class filter-class-1
```

Removing a Flow Filter Class:

```
switch(config-flow-ifa-initiator-monitor) # no flow-filter-class class-4
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context                   | Authority                                                                          |
|---------------|-----------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-flow-ifa-initiator-monitor | Administrators or local user group members with execution rights for this command. |

## flow ifa-initiator-monitor

```
flow ifa-initiator-monitor <NAME>
no flow ifa-initiator-monitor
```

### Description

Accesses the IFA initiator monitor context in the switch. This command creates a new IFA initiator monitor with the specified name.

The **no** form of this command exits the IFA initiator monitor context in the switch. It deletes the IFA initiator monitor with the specified name.

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <NAME>    | Specifies the IFA Monitor Initiator name. |

## Examples

Creating the Flow IFA initiator monitor **initiator-1**:

```
switch(config)# flow ifa-initiator-monitor initiator-1
```

Deleting the Flow Initiator monitor **initiator-2**

```
switch(config)# no flow ifa-initiator-monitor initiator-2
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## flow-telemetry-profile

```
flow-telemetry-profile
no flow-telemetry-profile
```

### Description

Accesses the Flow Telemetry Profile context in the switch.

The **no** form of this command resets all the Flow Telemetry Profile configuration to defaults.

### Examples

Accessing the Flow telemetry configuration context:

```
switch(config)# flow-telemetry-profile
```

Resetting all Flow Telemetry Profile settings to its defaults:

```
switch(config)# no flow-telemetry-profile
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## ifa-device-id

```
ifa-device-id {auto| <VALUE>}
no ifa-device-id {auto| <VALUE>}
```

### Description

Configures the IFA Device ID for the flow telemetry profile. The default setting is **auto** which configures the device identifier to match the low 20 bits of the switch's MAC address.

The **no** form of this command resets the IFA Device ID for the flow Telemetry Profile to the default value **auto**.

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| auto      | Resets the IFA Device ID of Flow Telemetry Profile to default.       |
| <VALUE>   | Specifies the interval range for IFA Device ID. Range: 0 to 1048575. |

### Examples

Configuring the IFA Device ID on the system:

```
switch(config-flow-telemetry-profile)# ifa-device-id 10
```

Configuring IFA Device ID **auto** on the system:

```
switch(config-flow-telemetry-profile)# ifa-device-id auto
```

Resetting the IFA Device ID for flow telemetry profile to default value **auto**:

```
switch(config-flow-telemetry-profile)# no ifa-device-id 10
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-flow-telemetry-profile | Administrators or local user group members with execution rights for this command. |

## ifa-hop-limit

```
ifa-hop-limit <VALUE>
no ifa-hop-limit <VALUE>
```

### Description

Configures the Inband Flow Telemetry (IFA) Hop Limit. The value used on IFA Metadata Header for created IFA probe packet running as the Initiator. Validate the number of IFA hops supported at the IFA Terminator node, before adjusting this value at the Initiator. In the case of AOS-CX, up to 10 IFA Hops are supported on a Terminator node.

The **no** form of this command resets the IFA hop limit to its default value.

| Parameter | Description                                                             |
|-----------|-------------------------------------------------------------------------|
| <VALUE>   | Specifies the IFA hop limit for the Flow Telemetry Profile. Default: 10 |

### Examples

Configuring the IFA hop limit on the system:

```
switch(config-flow-telemetry-profile)# ifa-hop-limit 10
```

Resetting the IFA Hop Limit value to the default value:

```
switch(config-flow-telemetry-profile)# no ifa-hop-limit
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-flow-telemetry-profile | Administrators or local user group members with execution rights for this command. |

## ifa-max-metadata-stack-length

```
ifa-max-metadata-stack-length <VALUE>
no ifa-max-metadata-stack-length <VALUE>
```

### Description

Configures the Inband Flow Telemetry Maximum Metadata Stack Length value in the IFA Metadata Header for created IFA probe packet running as the initiator. In the case of AOS-CX, only LNS 1 is supported. LNS 1 adds an IFA Metadata Stack with a size of 8 octets per hop.



Ensure that the IFA Max Metadata Stack Length aligns with the IFA hop limit value.

The **no** form of this command resets the IFA Max Metadata Stack Length for flow telemetry profile to its default value.

| Parameter | Description                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------|
| <VALUE>   | Specifies the maximum metadata stack length numeric value in multiples of four octets. The default value is 80. Range: 8 to 248. |

### Examples

Configuring the IFA Max Metadata Stack Length value on the system:

```
switch(config-flow-telemetry-profile)# ifa-max-metadata-stack-length 240
```

Resetting the IFA Max Metadata Stack Length for flow telemetry profile to the default value **80**:

```
switch(config-flow-telemetry-profile)# no ifa-max-metadata-stack-length
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

### Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-flow-telemetry-profile | Administrators or local user group members with execution rights for this command. |

## ifa-sampling-rate

```
ifa-sampling-rate <VALUE>
no ifa-sampling-rate <VALUE>
```

### Description

Configures the IFA sampling rate in multiples of a thousand packets to initiate cloned packets on filtered flows that match any configured initiator class, among all active IFA initiator monitors. For example, if the rate is set to 4, 1 out of every 4000 packets will be sampled.

The **no** form of this command resets the sampling rate to its default value.

| Parameter | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| <VALUE>   | Specifies the IFA sampling rate. The default value is 4. Range: 4 to 4200000. |

### Examples

Configure the IFA sampling rate for the flow telemetry profile:

```
switch(config-flow-telemetry-profile)# ifa-sampling-rate 240
```

Resetting the IFA sampling rate for the flow telemetry profile to its default value 4:

```
switch(config-flow-telemetry-profile)# no ifa-sampling-rate 240
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

### Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-flow-telemetry-profile | Administrators or local user group members with execution rights for this command. |

## ip-all flow ifa-terminator-monitor

```
ip-all flow ifa-terminator-monitor
no ip-all flow ifa-terminator-monitor
```

## Description

Applies the IFA terminator Monitor for all IP traffic. The IFA terminator monitor configuration is applied globally to the system, monitoring both IPv4 and IPv6 traffic. Only one role (transit or terminator) can be activated at a time. It overwrites the other command **ip-all flow ifa-transit-monitor** in case both are executed.

The **no** form of this command unconfigures the flow IFA terminator Monitor for all IP traffic.

## Examples

Applying the flow IFA terminator Monitor for all IP traffic:

```
switch(config)# ip-all flow ifa-terminator-monitor
```

Unconfiguring a Flow IFA terminator Monitor

```
switch(config)# no ip-all flow ifa-terminator-monitor
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## ip-all flow ifa-transit-monitor

```
ip-all flow ifa-transit-monitor
no ip-all flow ifa-transit-monitor
```

## Description

Applies the IFA Transit Monitor for all IP traffic probed by IFA. The IFA transit monitor configuration is applied globally to the system, monitoring both IPv4 and IPv6 traffic. Only one role (transit or terminator) can be activated at a time. It overwrites the other command **ip-all flow ifa-terminator-monitor** in case both are executed.

The **no** form of this command unconfigures the flow IFA Transit Monitor for all IP traffic.

## Examples

Applying the IFA Transit Monitor for all IP traffic:



```
switch(config)# ip-all flow ifa-transit-monitor
```

## Unconfiguring a Flow IFA Transit Monitor

```
switch(config)# no ip-all flow ifa-transit-monitor
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## {ip|ipv6} flow ifa-initiator-monitor

```
{ip|ipv6} flow ifa-initiator-monitor <NAME>
no {ip|ipv6} flow ifa-initiator-monitor <NAME>
```

## Description

Applies the IFA initiator monitor to the **config-if** or **config** context. IPv4 and IPv6 are supported. The monitor configuration should match the class IP version.

When a user has both system-level and port-level IFA initiator monitors, the port settings do not overwrite the system settings. Instead, both monitors work together. The system-initiator monitor samples packets to capture IFA probe packets, while any port-initiator monitors also operate simultaneously.



Supported contexts are system and interface

The **no** form of this command removes the IFA initiator monitor to the **config-if** or **config** context

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <NAME>    | Specifies the IFA Monitor Initiator name. |

## Examples

Applying the IFA Initiator Monitor to the system.

```
switch(config)# ip flow ifa-initiator-monitor initiator-1
```

```
switch(config)# ipv6 flow ifa-initiator-monitor initiator-1
```

Applying the IFA Initiator Monitor to a port range:

```
switch(config-if-<1/1/1-1/1/10>)# ip flow ifa-initiator-monitor initiator-1
```

```
switch(config-if-<1/1/1-1/1/10>)# ipv6 flow ifa-initiator-monitor initiator-1
```

Applying the IFA Initiator Monitor to a specific port:

```
switch(config-if-<1/1/1>)# ip flow ifa-initiator-monitor initiator-2
```

```
switch(config-if-<1/1/1>)# ipv6 flow ifa-initiator-monitor initiator-2
```

Removing the IFA Initiator Monitor to the system:

```
switch(config)# no ip flow ifa-initiator-monitor initiator-1
```

```
switch(config)# no ipv6 flow ifa-initiator-monitor initiator-2
```

```
switch(config)# no ip flow ifa-initiator-monitor
```

```
switch(config)# no ipv6 flow ifa-initiator-monitor
```

Removing the IFA Monitor Initiator to a port range:

```
switch (config-if-<1/1/1-1/1/10>)# no ip flow ifa-initiator-monitor initiator-1
```

```
switch (config-if-<1/1/1-1/1/10>)# no ip flow ifa-initiator-monitor
```

```
switch (config-if-<1/1/1-1/1/10>)# no ipv6 flow ifa-initiator-monitor initiator-1
```

```
switch (config-if-<1/1/1-1/1/10>)# no ipv6 flow ifa-initiator-monitor
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config<br>config-if | Administrators or local user group members with execution rights for this command. |

## show flow ifa metrics

show flow ifa metrics [brief]

### Description

Displays full information about current IFA flows. Timestamps are displayed in UTC. If **brief** is specified, then the flow IFA metrics summary is displayed.

### Examples

Showing flow IFA metrics summary:

```
switch# show flow ifa metrics brief
```

IFA metrics data will be available only if there is a local active IFA terminator. It can be validated with "show flow ifa monitor-status all"

| IP destination | IP source      | Dst port | Src port | IP protocol | VRF  |  |
|----------------|----------------|----------|----------|-------------|------|--|
| 10.10.100.2    | 10.10.10.5     | 2000     | 1000     | tcp         | <not |  |
| 2001:db8:3333  | DDDD:EEEE:FFFF | 8192     | 4096     | udp         | <not |  |
| 200:3::03      | 200:3::15      | 2000     | 1000     | tcp         | <not |  |
| 10.10.100.2    | 10.10.10.12    | 8192     | 4096     | udp         | <not |  |



The VRF is shown as **<not available>** because IFA is not performing VRF detection.

Showing flow IFA metrics on initiator or transit only node:

```
switch# show flow ifa metrics brief
```

IFA metrics data will be available only if there is a local active IFA terminator. It can be validated with "show flow ifa monitor-status all"

Showing flow IFA metrics on 9300 Switch Series::

```
switch# show flow ifa metrics
```

Total IFA packets Received: The number of IFA packets received for this flow that haven't been interrupted within a 5-minute time range.

Network IFA Path Latency: The cumulative latency across all IFA hops.

Egress Queue Depth Cells: Indicates the queue memory usage at the moment the IFA packet

passed through the switch. To determine the queue depth in bytes,

multiply this value by the block size 254 bytes.

Monitoring this alongside latency and link speed in the

IFA reports

can aid in predicting latency based on queue depth.

Congestion Packet Counter: A monotonically increasing counter indicating the number of packets,

out of the total received, that were marked as ECN-congested.

IFA metrics data will be available only if there is a local active IFA terminator. It can be validated with "show flow ifa monitor-status all"

Local IFA terminator metadata is not available. IFA metrics won't show local IFA hop.

```
Total IFA Packets Received: 20
Destination IP : 10.10.100.2
Source IP : 10.10.10.13
Destination Port : 8192
Source Port : 4096
IP Protocol : udp
VRF : <not available>
Network Path Latency : 1629 nanoseconds
ECN Congestion Hop : <None>
Max Hop Latency
 Device ID: 878080
 Latency : 875 nanoseconds
Terminator Timestamp : 2024-07-02 19:21:30 UTC
Number of Hops : 2
IFA Hop Path (Device ID) : 908765 -> 878080
```

| Device ID             | Ingress ASIC Port  | Egress ASIC Port | Egress Port        | Speed(Gbps)       | Egress Queue              |
|-----------------------|--------------------|------------------|--------------------|-------------------|---------------------------|
| Egress Queue TX Bytes | Egress Queue Depth | Cell             | Residence Time(ns) | RX Timestamp(UTC) | Congestion Packet Counter |

|            |     |    |     |   |            |
|------------|-----|----|-----|---|------------|
| 908765     | 255 | 26 | 40  | 1 |            |
| 7133048    | 1   |    | 754 |   | 2024-07-02 |
| 19:21:28 0 |     |    |     |   |            |
| 878080     | 62  | 34 | 40  | 1 |            |
| 8581664    | 1   |    | 875 |   | 2024-07-02 |
| 19:21:30 0 |     |    |     |   |            |

```
=====
=====
=====
```

Total IFA Packets Received: 916

```

Destination IP : 2001:db8:3333:4444:5555:6666:7777:8888
Source IP : 200:3::03
Destination Port : 2000
Source Port : 1000
IP Protocol : tcp
VRF : <not available>
Network Path Latency : 358433092 nanoseconds
ECN Congestion Hop : 908765
Max Hop Latency
 Device ID: 908765
 Latency : 358432202 nanoseconds
Terminator Timestamp : 2024-07-02 19:44:41 UTC
Number of Hops : 3
IFA Hop Path (Device ID) : 908765 -> 978670 -> 878080

Device ID Ingress ASIC Port Egress ASIC Port Egress Port Speed(Gbps) Egress Queue
Egress Queue TX Bytes Egress Queue Depth Cell Residence Time(ns) RX Timestamp(UTC)
Congestion Packet Counter

--
908765 255 26 40 1
84878144 200734 358432202 2024-07-02
19:44:38 915
978670 62 34 40 1
94820192 1 890 2024-07-02
19:44:40 915
878080 68 22 40 1
80317792 1 888 2024-07-02
19:44:41 915

```

Showing flow IFA metrics on 9300S Switch Series:

```

switch# show flow ifa metrics

Total IFA packets Received: The number of IFA packets received for this flow that
 haven not been interrupted within a 5-minute time
 range.
Network IFA Path Latency: The cumulative latency across all IFA hops

Egress Queue Depth Cells: Indicates the queue memory usage at the moment the IFA
packet
 passed through the switch. To determine the queue depth
 in bytes,
 multiply this value by the block size 318 bytes.
 Monitoring this alongside latency and link speed in the
IFA reports
 can aid in predicting latency based on queue depth.
Congestion Packet Counter: A monotonically increasing counter indicating the
number of packets,
 out of the total received, that were marked as ECN-
 congested.

IFA metrics data will be available only if there is a local active IFA terminator.
It can be validated with "show flow ifa monitor-status all"
Total IFA Packets Received: 20
Destination IP : 10.10.100.2
Source IP : 10.10.10.13
Destination Port : 8192
Source Port : 4096

```

IP Protocol : udp  
VRF : <not available>  
Network Path Latency : 1629 nanoseconds  
ECN Congestion Hop : <None>  
Max Hop Latency  
Device ID: 878080  
Latency : 875 nanoseconds  
Terminator Timestamp : 2024-07-02 19:21:30 UTC  
Number of Hops : 2  
IFA Hop Path (Device ID) : 908765 -> 878080

| Device ID             | Ingress ASIC Port  | Egress ASIC Port | Egress Port        | Speed(Gbps)       | Egress Queue |
|-----------------------|--------------------|------------------|--------------------|-------------------|--------------|
| Egress Queue TX Bytes | Egress Queue Depth | Cell             | Residence Time(ns) | RX Timestamp(UTC) |              |
| Congestion            | Packet             | Counter          |                    |                   |              |

|            |     |    |     |   |            |
|------------|-----|----|-----|---|------------|
| 908765     | 255 | 26 | 40  | 1 |            |
| 7133048    | 1   |    | 754 |   | 2024-07-02 |
| 19:21:28 0 |     |    |     |   |            |
| 878080     | 62  | 34 | 40  | 1 |            |
| 8581664    | 1   |    | 875 |   | 2024-07-02 |
| 19:21:30 0 |     |    |     |   |            |

=====  
=====  
=====

Total IFA Packets Received: 916  
Destination IP : 2001:db8:3333:4444:5555:6666:7777:8888  
Source IP : 200:3::03  
Destination Port : 2000  
Source Port : 1000  
IP Protocol : tcp  
VRF : <not available>  
Network Path Latency : 358433092 nanoseconds  
ECN Congestion Hop : 908765  
Max Hop Latency  
Device ID: 908765  
Latency : 358432202 nanoseconds  
Terminator Timestamp : 2024-07-02 19:44:41 UTC  
Number of Hops : 3  
IFA Hop Path (Device ID) : 908765 -> 978670 -> 878080

| Device ID             | Ingress ASIC Port  | Egress ASIC Port | Egress Port        | Speed(Gbps)       | Egress Queue |
|-----------------------|--------------------|------------------|--------------------|-------------------|--------------|
| Egress Queue TX Bytes | Egress Queue Depth | Cell             | Residence Time(ns) | RX Timestamp(UTC) |              |
| Congestion            | Packet             | Counter          |                    |                   |              |

|              |        |    |           |   |            |
|--------------|--------|----|-----------|---|------------|
| 908765       | 255    | 26 | 40        | 1 |            |
| 84878144     | 200734 |    | 358432202 |   | 2024-07-02 |
| 19:44:38 915 |        |    |           |   |            |
| 978670       | 62     | 34 | 40        | 1 |            |
| 94820192     | 1      |    | 890       |   | 2024-07-02 |
| 19:44:40 915 |        |    |           |   |            |
| 878080       | 68     | 22 | 40        | 1 |            |
| 80317792     | 1      |    | 888       |   | 2024-07-02 |
| 19:44:41 915 |        |    |           |   |            |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show flow ifa monitor-status all

```
show flow ifa monitor-status all
```

## Description

Displays information about currently configured IFA monitors.

## Examples

Showing flow IFA monitor-status on an initiator node with IPv4 and IPv6 configured and no ports configured:



The VRF is shown as **<not available>** because IFA is not performing VRF detection.

Showing flow IFA metrics on initiator or transit only node:

```
switch# show flow ifa monitor-status all

*** System ***

initiator_ipv4
 Target State : Active

initiator_ipv6
 Target State : Active
```

Showing flow IFA monitor-status on an initiator node with IPv4 and IPv6 configured and some ports are configured:

```
switch# show flow ifa monitor-status all

*** System ***

initiator_ipv4
 Target State : Active
```

```

initiator_ipv6
 Target State : Active

Port 1/1/1
initiator_ipv4
 Target State : Active

initiator_ipv6
 Target State : Programming

Port 1/1/4
initiator_ipv6
 Target State : Un-programming

Port 1/1/7
initiator_ipv4
 Target State : Active

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.15   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show running-config

```

show running-config [all | flow-telemetry-profile | current-context | flow ifa |
interface <INTERFACE-NAME >]

```

### Description

Shows the current running configuration.

### Examples

Showing all the running configuration:

```

switch# show running-config all
Current configuration:
!
!
flow-telemetry-profile
 ifa-device-id auto

```



```
ifa-hop-limit 10
ifa-max-metadata-stack-length 80
ifa-sampling-rate 4
```

Showing the flow-telemetry-profile configuration:

```
switch# show running-config flow-telemetry-profile

flow-telemetry-profile
 ifa-device-id 30
 ifa-hop-limit 55
 ifa-max-metadata-stack-length 90
 ifa-sampling-rate 13
```

Show running configuration after configuring some IFA initiator monitors to the system:

```
switch# show running-config flow ifa

Current configuration:
!
!
class ifa-ip class-ifa
class ifa-ipv6 class-ifa-ipv6
flow ifa-initiator-monitor ifa-init
 flow-filter-class class-ifa
flow ifa-initiator-monitor ifa-init2
 flow-filter-class class-ifa-ipv6
flow ifa-initiator-monitor ifa-init3
```

Show running configuration after configuring IFA initiator monitor to a specific port:

```
switch# show running-config flow ifa

Current configuration:
!
!
flow ifa-initiator-monitor ifa-init-port
interface 1/1/1
 ip flow ifa-initiator-monitor ifa-init-port
```

Show running configuration after configuring IFA initiator monitor to a port range:

```
switch# show running-config flow ifa

Current configuration:
!
!
flow ifa-initiator-monitor ifa-init-port
interface 1/1/1
 ip flow ifa-initiator-monitor ifa-init-port
interface 1/1/2
 ip flow ifa-initiator-monitor ifa-init-port
interface 1/1/3
 ip flow ifa-initiator-monitor ifa-init-port
interface 1/1/4
 ip flow ifa-initiator-monitor ifa-init-port
```

```
interface 1/1/5
 ip flow ifa-initiator-monitor ifa-init-port
```

Show running with IFA Monitor configuration combined:

```
switch# show running-config

Current configuration:
!
!
class ifa-ip class-ifa
class ifa-ipv6 class-ifa-ipv6
flow ifa-initiator-monitor ifa-init-ipv6
 flow-filter-class class-ifa-ipv6
flow ifa-initiator-monitor ifa-init
 flow-filter-class class-ifa
ip-all ifa-transit-monitor
ip flow ifa-initiator-monitor ifa-init
ipv6 flow ifa-initiator-monitor ifa-init-ipv6
interface 1/1/1
 ip flow ifa-initiator-monitor ifa-init
interface 1/1/2
 ipv6 flow ifa-initiator-monitor ifa-init-ipv6
interface 1/1/3
 ip flow ifa-initiator-monitor ifa-init
 ipv6 flow ifa-initiator-monitor ifa-init-ipv6
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.15   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### ip igmp snooping all-vlans

ip igmp snooping all-vlans  
no ip igmp snooping all-vlans

#### Description

Enable IGMP snooping on all VLANs. This configuration setting enables IGMP snooping on all existing VLANs, as well as on any VLANs that are created after the **ip igmp snooping all-vlans** command is issued. When IGMP snooping is enabled globally, IGMP snooping can not be configured on individual VLANs within the VLAN context of the command-line interface.

The **no** form of this command disables global IGMP snooping, allows IGMP snooping to remain enabled at the VLAN level, and allows the configuration of VLAN-level IGMP snooping settings.

#### Example

Configure IGMP snooping globally:

```
switch(config)# ip igmp snooping all-vlans
```

Disable global IGMP snooping:

```
switch(config)# no ip igmp snooping all-vlans
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

#### Command History

| Release    | Modification        |
|------------|---------------------|
| 10.16.1000 | Command introduced. |

#### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

### ip igmp snooping apply access list

ip igmp snooping apply access list <ACL-NAME>

```
no ip igmp snooping apply access list <ACL-NAME>
```

## Description

Configures the access list (ACL) in a particular interface to filter IGMP join or leave packets based on rules set in a particular access list name. The **no** form of this command removes the configuration.

| Parameter  | Description                     |
|------------|---------------------------------|
| <ACL-NAME> | Specifies the access list name. |

## Usage

Existing classifier commands are used to configure ACL. In case of IGMPv3 packets with multiple group addresses received, only permitted group addresses based on the ACL rule set are processed. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL to avoid the delay in learning of the permitted groups because the access switch configured with the ACL blocks the traffic for the groups which are denied forwarding of joins have no impact. If all of the groups in a packet are denied by the ACL rule packet, it is not forwarded to the querier and PIM router. If the ACE has the source address configured, the source address in the IGMPv3 report is matched against the ACL and corresponding action is taken. Existing joins timeout.

With IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.



If the access list is configured for both L2 VLAN and L3 VLAN, then the L3 VLAN configuration is applied.

## Example

Configure the access list:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping apply access-list mygroup
```

Remove the access list:

```
switch(config)# vlan 2
switch(config-vlan-2)# no ip igmp snooping apply access-list mygroup
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.13   | Command introduced. |

## Command Information

| Platforms    | Command context | Authority                                                                          |
|--------------|-----------------|------------------------------------------------------------------------------------|
| All platform | config-vlan     | Administrators or local user group members with execution rights for this command. |

## ip igmp snooping querier-address

```
ip igmp snooping querier-address <QUERIER-IP-ADDRESS>
no ip igmp snooping querier-address <QUERIER-IP-ADDRESS>
```

### Description

Configures the querier IP address for the IGMP-MLD proxy feature in EVPN. The **no** form of this command removes the configuration.

| Parameter            | Description                             |
|----------------------|-----------------------------------------|
| <QUERIER-IP-ADDRESS> | Specifies the proxy querier IP address. |

### Usage

Fabrics running the IGMP-MLD Proxy feature must perform distributed querier functionality on every VTEP where the VLAN is extended. Typically, a valid IP address must be configured on the SVI for IGMP querier functionality. However, in centralized routing scenarios within the fabric, most VTEPs only have Layer 2 VLANs. In such cases, IGMP querier functionality needs to be enabled on those VTEPs. This configuration provides a valid querier IP address for those Layer 2 VLANs.

This command is used in conjunction with the IGMP-MLD proxy feature of EVPN.



This is an optional command applicable to VTEPs that have Layer 2 VLANs (without an IP address) and requires IGMP-MLD proxy querier functionality.

If a Layer 3 SVI with an IP address is configured for the VLAN, it takes precedence. In the absence of a valid IP address or SVI, the given IP address is used for querier operations. This configuration is global and applies to all tenants' Layer 2 VLANs where the IGMP-MLD proxy feature is enabled. Fabrics running the **igmp-mlD proxy** feature must perform distributed querier functionality on every VTEP where the VLAN is extended. Typically, a valid IP address must be configured on the SVI for IGMP querier functionality needs to be enabled on those VTEPs. This configuration provides a valid querier IP address for those Layer 2 VLANs. This configuration is applicable only when **igmp-mlD-proxy** configuration is configured under EVPN.

In the event of underlay tunnel fluctuations, the querier state reinitializes and transitions back to the querier state only after the default querier wait of 260 seconds.

This configuration is not applicable to VLANs that are not mapped to a VNI.



The specified IP address does not need to be assigned to any interface.

### Example

Configure the querier IP address for the IGMP-MLD proxy feature in EVPN.

```
switch(config)# ip igmp snooping querier-address 10.10.10.1
```

Remove the configuration of the querier IP address for the IGMP-MLD proxy feature in EVPN:

```
switch(config)# no ip igmp snooping querier-address 10.10.10.1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms    | Command context | Authority                                                                          |
|--------------|-----------------|------------------------------------------------------------------------------------|
| All platform | config          | Administrators or local user group members with execution rights for this command. |

## ip igmp snooping static group

```
ip igmp snooping static group <GROUP-NAME>
no ip igmp snooping static group <GROUP-NAME>
```

## Description

Configures static multicast group. The **no** form of this command removes the configuration.

| Parameter    | Description               |
|--------------|---------------------------|
| <GROUP-NAME> | Specifies the group name. |

## Example

Configure static multicast group on group 239.1.1.1:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping static-group 239.1.1.1
```

Remove static multicast group on group 239.1.1.1:

```
switch(config)# vlan 2
switch(config-vlan-2)# no ip igmp snooping static-group 239.1.1.1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.13   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-vlan     | Administrators or local user group members with execution rights for this command. |

## ip igmp snooping (config mode)

```
ip igmp snooping
drop-unknown vlan-shared|vlan-exclusive
fastlearn <PORT-LIST>
```

### Description

Configures drop-unknown and fastlearn modes on the ports. While IGMP snooping is enabled, the traffic will be forwarded only to ports that made an IGMP request for the multicast. Drop unknown filters ensure that packets are not forwarded to ports that did not make a request for the traffic stream. This could either be a filter across all VLANs (**vlan-shared**) or per VLAN (**vlan-exclusive**). The default is **vlan-shared**. Fast learn enables the port to learn group information when receiving a topology change notification. By default, fast learn is not enabled on ports.

| Parameter             | Description                                                                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| drop-unknown          | Drop unknown filters ensure that packets are not forwarded to ports that did not make a request for the traffic stream.                                                                                                                                             |
| vlan-shared           | Enables a shared VLAN filter on the switch. Default is <b>vlan-shared</b> .                                                                                                                                                                                         |
| vlan-exclusive        | Enables an exclusive drop unknown filter per VLAN.                                                                                                                                                                                                                  |
| fastlearn <PORT-LIST> | Enable fast learn on ports. This parameter specifies a list of one or more ports to be configured as fast learn ports. You can specify a single port, a comma-separated list of ports or a range of ports such as 1/1/1-1/1/3. You may also enter an L2 LAG (1-128) |
| no ...                | Negates any configured parameter.                                                                                                                                                                                                                                   |

### Example

Configuring fast learn ports:

```
switch(config)# ip igmp snooping fastlearn 1/1/3
switch(config)# ip igmp snooping fastlearn 1/1/1-1/1/2
switch(config)# ip igmp snooping fastlearn 1/1/5,1/1/6
```

Configuring a shared VLAN filter on the switch:

```
switch(config)# ip igmp snooping drop-unknown vlan-shared
```

Configuring a exclusive drop unknown filter per VLAN:

```
switch(config)# ip igmp snooping drop-unknown vlan-exclusive
```

Disabling drop unknown on the switch:

```
switch(config)# no ip igmp snooping drop-unknown
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip igmp snooping (interface mode)

```
ip igmp snooping
 auto vlan <VLAN-LIST>
 blocked vlan <VLAN-LIST>
 fastleave vlan <VLAN-LIST>
 forced-fastleave vlan <VLAN-LIST>
 forward vlan <VLAN-LIST>
 no ...
```

## Description

Configure IP IGMP snooping for the VLAN on the interface. When IGMP snooping is enabled, the L2 snooping switch forwards multicast packets of known multicast groups to only the receivers. When IGMP snooping is not enabled, the snooping switch floods multicast packets to all hosts on the VLAN.

| Parameter             | Description                                                                                                                                                                                                                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auto vlan <VLAN-LIST> | Instruct the device to monitor incoming multicast traffic on the specified ports on a VLAN or VLAN range. This is the default behavior. Enter the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60). |



| Parameter                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>blocked vlan &lt;VLAN-LIST&gt;</code>          | Configures the specified ports in blocked mode for the specified VLAN list. In blocked mode, joins and traffic are always blocked on this port. Enter the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>fastleave vlan &lt;VLAN-LIST&gt;</code>        | <p>IGMP fastleave is configured for ports on a per-VLAN basis. Upon receiving a Leave Group message, the querier sends an IGMP Group-Specific Query message out of the interface to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host.</p> <p>When a fastleave-enabled switch port is connected to a single host and receives a leave, the switch does not wait for the querier status update interval, but instead immediately removes the IGMP client from its IGMP table and ceases transmitting multicast traffic to the client. (If the switch detects multiple end nodes on the port, Fastleave does not activate regardless of whether one or more of these end nodes are IGMP clients.) This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an IGMP Group-Specific Query message.</p> <p>This parameter specifies a list of VLANs on which the port should be configured as a fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).</p> |
| <code>forced-fastleave vlan &lt;VLAN-LIST&gt;</code> | <p>With forced fastleave enabled, IGMP speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits for a second to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port.</p> <p>This parameter specifies a list of VLANs on which the port should be configured as a forced fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).</p> <p>This command is available in <b>config-if</b> mode.</p>                                                                                                                                                                                                                                                                                                                                                               |
| <code>forward vlan &lt;VLAN-LIST&gt;</code>          | <p>Configures the specified ports in forward mode in the given VLAN list. In forward mode, traffic is always forwarded on this port, irrespective of joins. Specify a list of VLANs on which the port should be configured as a forward port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).</p> <p>This command is available in <b>config-if</b> mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>no ...</code>                                  | Negates any configured parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Example

Configure auto ports for VLAN on the interface:

```

switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping auto vlan 10
switch(config-if)# ip igmp snooping auto vlan 10-20

```

Configuring fastleave ports for the VLAN on the interface:

```

switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping fastleave vlan 10
switch(config-if)# ip igmp snooping fastleave vlan 10-20

```

Configuring blocked ports for the VLAN on the interface:

```

switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping blocked vlan 10
switch(config-if)# ip igmp snooping blocked vlan 10-20

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## ip igmp snooping (vlan mode)

```

ip igmp snooping
 apply access-list <ACL-NAME>
 enable|disable
 no ...
 static-group <MULTICAST-IP-ADDRESS>
 version <2-3> (vlan interface mode)

```

## Description

These commands enable or disable IP IGMP snooping on the VLAN, create IGMP snooping static multicast groups, set the IGMP snooping version and configure the ACL on a particular interface.



Disabling and enabling IGMP snooping on a VLAN causes IGMP querier re-election.

| Parameter                                              | Description                                                                                                                                                                                     |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-list</code>                               | Associates an ACL with the IGMP.                                                                                                                                                                |
| <code>enable disable</code>                            | Enables or disables IGMP snooping on the VLAN. Starting with AOS-CX 10.16, IGMP snooping is enabled by default.                                                                                 |
| <code>no ...</code>                                    | Negates any configured parameter.                                                                                                                                                               |
| <code>static-group &lt;MULTICAST-IP-ADDRESS&gt;</code> | This parameter configures an IGMP snooping static multicast group. Specify the IGMP static multicast group IP address in A.B.C.D format. You can configure a maximum of 32 IGMP snooping static |
| <code>version &lt;2-3&gt;</code>                       | Configures the IGMP snooping version on the VLAN. Select <b>2</b> for IGMPv2 (RFC2236). Select <b>3</b> for IGMPv3 (RFC3376).                                                                   |

## Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by the ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.



If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

## Example

Disable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping disable
```

Reenable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping enable
```

Configuring an IGMP snooping static group:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping static-group 239.1.1.1
switch(config-vlan)# no ip igmp snooping static-group 239.1.1.1
```

Configuring IGMP snooping version on the VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping version 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release          | Modification                                                                                                                                      |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 10.16            | Starting with this release, IGMP snooping is enabled on VLANs by default, including the Management VLAN (vlan 1) and VLANs with a associated VNI. |
| 10.07 or earlier | --                                                                                                                                                |

## Command Information

| Platforms     | Command context       | Authority                                                                          |
|---------------|-----------------------|------------------------------------------------------------------------------------|
| All platforms | config-vlan-<VLAN-ID> | Administrators or local user group members with execution rights for this command. |

## show ip igmp snooping

```
show ip igmp snooping
 counters
 detail
 groups [vlan <vlan-id>]
 no ...
 packet-exceptions
 static-groups
 statistics
 vlan <vlan-id> [group {<ip-addr> [client_details]}|{port <IF-NAME>}|{vtep-peer <A.B.C.D>}]
 vsx-peer
```

## Description

Shows IGMP snooping configuration information and status for all VLANs. Specify a VLAN ID or a VLAN and a group to display details for only that VLAN or VLAN group.

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| counters  | Shows IGMP query packets transmitted (Tx), received (Rx), and |

| Parameter                  | Description                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | error packet counters.                                                                                                                                                                                                           |
| detail                     | Shows IGMP Snooping details for all VLANs, including joined ports or VXLAN tunnel endpoints (VTEPs) for each group in the VLAN.                                                                                                  |
| groups                     | Shows IGMP snooping groups information. Include the optional <b>vlan &lt;vlan-id&gt;</b> parameter to display information for groups on a specific VLAN.                                                                         |
| no ...                     | Negates any configured parameter.                                                                                                                                                                                                |
| packet-exceptions          | Troubleshoot issues in L2 multicast bridge entries for data packets forwarded to the CPU.                                                                                                                                        |
| static-groups              | Shows MLD snooping static group details, including the number of static groups joined.                                                                                                                                           |
| statistics                 | Shows MLD snooping statistics.                                                                                                                                                                                                   |
| vlan <vlan-id>             | Shows IGMP snooping protocol information and number of different groups joined for the VLAN.                                                                                                                                     |
| group                      | Shows IGMP snooping group information for the specified VLAN, including the number of different groups joined for the VLAN. Identify the group by IP address or interface name.                                                  |
| <ip-addr> [client-details] | Shows IGMP snooping group address information. Include the optional <b>client details</b> parameter to display IGMP snooping client details.                                                                                     |
| port <IF-NAME>             | Shows IGMP snooping group information for the interface name in <b>member/slot/port</b> format.                                                                                                                                  |
| vtep-peer <A.B.C.D>        | Shows IGMP snooping info for the specified VTEP.                                                                                                                                                                                 |
| vsx-peer                   | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing IGMP snooping configuration and status:

```
switch# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled : 1
IGMP Drop Unknown Multicast : Global
Configured IGMP Proxy Querier address : 10.10.10.1

VLAN ID : 1
VLAN Name : DEFAULT_VLAN_1
IGMP Snooping is not enabled

VLAN ID : 2
```

```

VLAN Name : VLAN2
IGMP Configured Version : 3
IGMP Operating Version : 3
IGMP preprogram-starg-flow is operational
Querier Address [this switch] : 20.1.1.1
Querier Port :
Querier UpTime :0m 21s
Querier Expiration Time :0m 2s

```

Include the **detail** parameter for additional information on joined ports or VTEPs, as shown in the example below:

```

switch# show ip igmp snooping detail

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled : 1
Current count of multicast groups joined : 4

IGMP Drop Unknown Multicast : Global
VLAN ID : 100
VLAN Name : VLAN100
IGMP Configured Version : 3
IGMP Operating Version : 3
IGMP preprogram-starg-flow is not operational
Querier Address [this switch] : 15.1.1.1
Querier Port :
Querier UpTime :9m 32s
Querier Expiration Time :0m 10s
Router Detected Port(s) :

Active Group Address Tracking Vers Mode Uptime Expires Ports/Vteps

225.1.1.1 Filter 3 EXC 1m 2s 0s
200.1.1.1,200.1.1.2
1/6/22
225.1.1.2 Filter 3 EXC 1m 2s 0s
200.1.1.1,200.1.1.2
1/6/22
226.1.1.1 Filter 3 EXC 1m 4s 0s
200.1.1.3
226.1.1.2 Filter 3 EXC 1m 4s 0s
200.1.1.3

```



With standard based IGMP-MLD Proxy mode, the membership reports from remote VTEPs does not have an expiry timer associated and shall be shown as 0 seconds.



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification                                               |
|---------|------------------------------------------------------------|
| 10.16   | Updated example to include new IGMP proxy querier address. |

| Release          | Modification                                          |
|------------------|-------------------------------------------------------|
| 10.13            | Programming starg flow is now supported.              |
| 10.10            | The <b>packet-exceptions</b> parameter is introduced. |
| 10.07 or earlier | --                                                    |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## clear update-log

```
clear update-log
```

### Description

Clears stored log files of any In-System Programming updates on the system.



---

For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

---

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show needed-updates

```
show needed-updates [next-boot [primary|secondary]]
```

### Description

Displays whether any programmable devices are in need of an update.

Without the **next-boot** parameter, this command displays needed updates relative to the currently running AOS-CX image.

With the **next-boot** parameter, this command displays needed updates relative to an AOS-CX image file in the persistent storage of the switch, which might be different from the currently running image. If either the **primary** or **secondary** parameter is specified, this command queries that specific AOS-CX image file. Otherwise, it queries the default AOS-CX image file as set by the most recent **boot system** or **boot set-default** command.



---

For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

---

### Command History



| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## allow-unsupported-transceiver

```
allow-unsupported-transceiver [confirm | log-interval {none | <INTERVAL>}]
no allow-unsupported-transceiver
```

### Description

Allows unsupported transceivers to be enabled or establish connections. Transceivers with speeds up to 100G are enabled by this command.

- The following models will enable unsupported transceivers for speeds up to 100G when running AOS-CX 10.09.0001 or later:
  - 8325 (Models 48Y8C and 32C)
  - 8360 (Models 48Y6C, 32Y4C, 16Y2C, 48XT4C, 24XF2C and 12C)
  - 9300, 9300S Series Switches
  - 10000 Series Switches
- The 8320 Series Switches will enable unsupported transceivers for speeds up to 40G when running AOS-CX 10.10 or later.

This command is enabled by default, allowing the use of third party transceiver products without adding the command in the configuration. Disabling this command with the **no** form will now disable the command in the running and stored configurations.

The **no** form of this command disallows using unsupported transceivers.

| Parameter               | Description                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------|
| confirm                 | Specifies that unsupported transceiver warnings are to be automatically confirmed.                                 |
| log-interval none       | Disables unsupported transceiver logging.                                                                          |
| log-interval <INTERVAL> | Sets the unsupported transceiver logging interval in minutes. Default: 1440 minutes. Range: 1440 to 10080 minutes. |

### Usage

When none of the parameters are specified it will display a warning message to accept the warranty terms. With **confirm** option the warning message is displayed but the user is not prompted to **(y/n)** answering. Warranty terms must be agreed to as part of enablement and the support is on best effort basis.

## Examples

Allowing unsupported transceivers with follow-up confirmation:

```
switch(config)# allow-unsupported-transceiver
Warning: The use of unsupported transceivers, DACs, and AOCs is at your
own risk and may void support and warranty. Please see HPE Warranty terms
and conditions.

Do you agree and do you want to continue (y/n)? y
```

Allowing unsupported transceivers with confirmation in command syntax:

```
switch(config)# allow-unsupported-transceiver confirm
Warning: The use of unsupported transceivers, DACs, and AOCs is at your
own risk and may void support and warranty. Please see HPE Warranty terms
and conditions.
```

Configuring unsupported transceiver logging with an interval of every 48 hours:

```
switch(config)# allow-unsupported-transceiver log-interval 2880
```

Disabling unsupported transceiver logging:

```
switch(config)# allow-unsupported-transceiver log-interval none
```

Disallowing unsupported transceivers with follow-up confirmation:

```
switch(config)# no allow-unsupported-transceivers
Warning: Unsupported transceivers, DACs, and AOCs will be disabled,
which could impact network connectivity. Use 'show allow-unsupported-transceiver'
to identify unsupported transceivers, DACs, and AOCs.

Continue (y/n)? y
```

Disallowing unsupported transceivers with confirmation in command syntax:

```
switch(config)# no allow-unsupported-transceiver confirm
Warning: Unsupported transceivers, DACs, and AOCs will be disabled,
which could impact network connectivity. Use 'show allow-unsupported-transceiver'
to identify unsupported transceivers, DACs, and AOCs.

switch(config)#
```



---

For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| all platforms | config          | Administrators or local user group members with execution rights for this command. |

## default interface

default interface <INTERFACE-ID>

### Description

Sets an interface (or a range of interfaces) to factory default values.

| Parameter      | Description                                                                                                                                                    |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-ID> | Specifies the ID of a single interface or range of interfaces. Format: <b>member/slot/port</b> or <b>member/slot/port-member/slot/port</b> to specify a range. |

### Examples

Resetting an interface:

```
switch(config)# default default interface 1/1/1
```

Resetting an range of interfaces:

```
switch(config)# default default interface 1/1/1-1/1/10
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# description

description <DESCRIPTION>  
no description

## Description

Associates descriptive information with an interface to help administrators and operators identify the purpose or role of an interface.

The **no** form of this command removes a description from an interface.

| Parameter     | Description                                                                                                          |
|---------------|----------------------------------------------------------------------------------------------------------------------|
| <DESCRIPTION> | Specify a description for the interface. Range: 1 to 64 ASCII characters (including space, excluding question mark). |

## Examples

Setting the description for an interface to **DataLink 01**:

```
switch(config-if) # description DataLink 01
```

Removing the description for an interface.

```
switch(config-if) # no description
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

# error-control

error-control {auto | none | base-r-fec | rs-fec}  
no error-control {auto | none | base-r-fec | rs-fec}

## Description

Configures the forward error correction (FEC) mode to use for an interface. When not configured, the system will automatically select the FEC mode based on the installed transceiver. In most cases, the standard FEC mode will work best, but certain link partners may require a non-standard mode.

The **no** and **auto** forms of this command configure the interface to automatically use the standard FEC mode of the currently installed transceiver.



FEC configuration only applies to transceivers, DACs, or AOCs running at 25G or 100G. 100G DACs are a special case. They can only set FEC to none when auto-negotiation is disabled through the **speed override** command. The default for the installed transceiver is used in all other cases.



Transceivers for which FEC is auto-negotiated will request the mode configured by this command, but may resolve to a different mode. The applied FEC mode is displayed as a commented line in the configuration shown with the **show run** command. It is also displayed with **show interface** command.

| Parameter  | Description                     |
|------------|---------------------------------|
| auto       | Use the transceiver default.    |
| none       | Do not use any FEC.             |
| base-r-fec | Use IEEE BASE-R (Firecode) FEC. |
| rs-fec     | Use IEEE RS (Reed-Solomon) FEC. |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification        |
|------------|---------------------|
| 10.08.1021 | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## flow-control

On the 9300/9300S,:

```
flow-control {rx | rxtx [pool <POOL-NUM>]}
no flow-control {rx | rxtx [pool <POOL-NUM>]}
flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
```

```
no flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
```

**Note:** Up to three priority lists in the same command are supported, one each for `rxtx`, `rx`, and `tx`.

## Description

On the 8100, 8325, 8360, 9300/9300S, and 10000, **flow-control** enables negotiation of either receive-only flow control or both receive and transmit flow control on the current interface. The switch advertises either RX or RXTX support to the link partner. The final configuration is determined based on the capabilities of both partners.

On the 8100, 8325, 8360, 9300/9300S, and 10000, **flow-control priority** enables priority-based flow control (PFC). Multiple priorities are supported. Bidirectional (symmetric) PFC is configured with parameter **priority rxtx**. Unidirectional (asymmetric) PFC is configured with either parameter **priority rx** or **priority tx**.

On the 8100, 8325, 8360, 9300/9300S, and 10000, when configuring PFC for multiple priority levels, the complete list of priorities must be specified in a single command. Priorities cannot be added or subtracted using separate commands.

Each invocation of this command replaces the previous configuration.

The **no** form of these commands disables any configured flow control on the selected interface.

| Parameter                                 | Description                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>rx</code>                           | Enables the ability to cease and resume transmission when receiving IEEE 802.3x LLFC pause frames on this interface.                                                                                                                                                                                                                 |
| <code>rxtx [pool &lt;POOL-NUM&gt;]</code> | (Applies to the 8325, 9300/9300S, 10000.) <b>rxtx</b> enables the ability to honor received and to transmit IEEE 802.3x LLFC pause frames to the remote device.<br><b>pool &lt;POOL-NUM&gt;</b> optionally selects the number of the lossless pool used for buffering packets arriving on this interface. Default: 1. Range: 1 to 3. |
| <code>priority rxtx</code>                | (Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enables the ability to honor received and to transmit IEEE 802.1Qbb PFC pause frames on the interface for the configured packet priority.                                                                                                                                      |
| <code>priority rx</code>                  | (Applies to the 8325, 9300/9300S, 10000.) Enables the ability to honor received IEEE 802.1Qbb PFC pause frames on the interface for the configured packet priorities. This can be useful for implementing asymmetric PFC when it is desired to configure this only in the receive direction.                                         |
| <code>priority tx</code>                  | (Applies to the 8325, 9300/9300S, 10000.) Enables the ability to transmit IEEE 802.1Qbb PFC pause frames on the interface for the configured packet priorities. This can be useful for implementing asymmetric PFC when it is desired to configure this only in the transmit direction.                                              |
| <code>&lt;PRIORITY-LIST&gt;</code>        | (Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Specifies a comma-separated list of packet priorities for which PFC will operate. Range: 0 to 7. Up to seven priorities (two on the 8100 and 8360) can be specified in the list.                                                                                               |

## Usage (flow control)

- For interfaces that auto-negotiate, link-level flow control is subject to negotiation, plus speed and other parameters. Both ends of the link must negotiate the same flow control mode for it to be applied.
- For interfaces that do not auto-negotiate, the configured link-level flow control mode is always applied and the user is responsible for ensuring that both ends of the link are configured for the same mode.
- All members of a LAG must have the same flow control configuration.
- Lossless flow control is only supported for single destination unicast traffic. Replicated traffic (for example, broadcast, multicast, mirroring) cannot be guaranteed to be lossless.
- Lossless behavior is not supported when operating in a VSF stack configuration.

## Usage (priority-based flow control (PFC))

- PFC will only operate correctly between interfaces with the same priority configuration. Traffic flow will not be lossless between interfaces with different priorities or between interfaces where one has PFC enabled and the other does not.
- On the 8325, 9300/9300S, 10000, PFC takes effect after the configuration is saved and the switch is restarted.
- On the 8325, 9300/9300S, 10000, lossless pools must be created before configuring flow control on any interface. For PFC (when the PFC mode includes TX), any priority to be configured for PFC must be mapped to a lossless pool before it can be enabled for PFC. For link-level flow control, lossless pool 1 will be used by default if no pool is specified when enabling flow control on the interface. If a pool is specified when enabling flow control on an interface, the specified pool must be created first before enabling flow control.
- Any queue used by protocol or control traffic must not be configured for lossless behavior. Routing protocols and VSX-synchronization messages use local-priority 7, therefore the CoS priority mapped to local-priority 7 should not be used in any lossless configuration.  
For example, in a default configuration, the CoS map assigns local-priority 7 to packets arriving with VLAN priority 7. This means that lossless pools should not be configured to use priority 7, and that any `flow-control priority` mode should not be configured on priority 7, since that VLAN priority maps to local-priority 7.
- On the 8325, 9300/9300S, 10000, whatever lossless pool(s) will be used for link-level flow control must be created before configuring link-level flow control RXTX mode on any interface. Otherwise, a message similar to the following will be displayed:

```
Lossless pool 1 must be configured using the 'qos pool' command before enabling
RXTX flow control.
```

- On the 8325, 9300/9300S, 10000, link-level flow control RXTX mode is not subject to auto-negotiation. It is recommended to configure PFC or link-level flow control RXTX mode and pools only once on a running system. Changing the pool or flow control configuration on a running system will cause a brief disruption in traffic. The reconfiguration also results in packet loss in the data flow. This may affect one, multiple, or all ports depending on the existing configuration and changes made to it.



---

On the 8325, 9300/9300S, and 10000:

You can only apply three unique combinations of PFC priority configuration across all ports of a switch.

**For example:**

```
flow-control priority 3
flow-control priority 4,5
flow-control priority 4
```

The first three unique combinations configured across all ports sorted in numerical order are accepted and applied. If you attempt to configure a fourth unique priority combination, the following error message is displayed:

The number of unique priority-based flow control (PFC) configuration combinations cannot be more than 3.

Note that ports with a PFC configuration that cannot be applied can still link up but they will not have any flow control.

---

## Examples

Enabling support for RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control rx
```

Disabling support for RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control rx
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control txrx
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Disabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control txrx
```

(Applies to the 8325, 9300/9300S, 10000.) Enabling support for RXTX flow control with pool setting:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control rxtx pool 2
```

(Applies to the 8325, 9300/9300S, 10000.) Disabling support for RXTX with pool setting:

```
switch(config)# interface 1/1/1
```

```
switch(config-if) # no flow-control rxtx pool 2
```

(Applies to the 8325, 9300/9300S, 10000.) Enabling support for priority RX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # flow-control priority rx 3,4
```

(Applies to the 8325, 9300/9300S, 10000.) Disabling support for priority RX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # no flow-control priority rx 3,4
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enabling support for priority RXTX and RX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # flow-control priority rxtx 3 rx 1,2,4,5,6
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Disabling support for priority RXTX and RX flow control:

(Applies to the 8325, 9300/9300S, 10000.) Enabling support for priority TX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # flow-control priority tx 3,4
```

(Applies to the 8325, 9300/9300S, 10000.) Disabling support for priority TX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # no flow-control priority tx 3,4
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enabling support for priority RXTX, RX, and TX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # flow-control priority rxtx 3 rx 1,2,4 tx 5,6
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Disabling support for priority RXTX, RX, and TX flow control:

```
switch(config) # interface 1/1/1
switch(config-if) # no flow-control priority rxtx 3 rx 1,2,4 tx 5,6
```



---

For more information on how to use this command, refer to the Fundamentals Guide for your switch model.

---

## Command History

| Release          | Modification                                                                                                       |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| 10.10            | Adjusted the priority syntax. Added separate RX and TX configuration for asymmetric PFC. Added the pool parameter. |
| 10.08            | Command enhanced to configure two PFC priorities.                                                                  |
| 10.07 or earlier | --                                                                                                                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## flow-control buffer headroom

```

flow-control buffer priority <PRIORITY> headroom <LIMIT> kbytes
flow-control buffer llfc headroom <LIMIT> kbytes
no flow-control buffer priority <PRIORITY> headroom <LIMIT> kbytes
no flow-control buffer llfc headroom <LIMIT> kbytes

```

### Description

Allows user configuration of per-priority or LLFC RXTX headroom limit on a physical interface. The **no** form of the command resets the limit to the default value.

| Parameter                              | Description                                                                                                                                                                                |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>priority &lt;PRIORITY&gt;</code> | Configures buffer parameters for priority flow control. Range: 0 to 7.                                                                                                                     |
| <code>llfc</code>                      | Configures buffer parameters for link-level flow control.                                                                                                                                  |
| <code>headroom &lt;LIMIT&gt;</code>    | Specifies the maximum amount of headroom pool buffer space that is allowed to be used for in-flight packets that arrive after flow-control XOFF is asserted. Range: 18 to 10240 kilobytes. |

### Examples

Configuring a headroom limit of 36 kbytes for PFC priority 4 traffic:

```

switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 4 headroom 36 kbytes

```

Configuring a headroom limit of 36 kbytes for LLFC RXTX traffic:

```

switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc headroom 36 kbytes

```

Resetting the headroom limit to default value:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 4 headroom 36 kbytes
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                            |
|---------|-----------------------------------------|
| 10.11   | Added support for 9300 series switches. |
| 10.10   | Command Introduced.                     |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config-if       | Administrators or local user group members with execution rights for this command. |

## flow-control buffer xon

```
flow-control buffer priority <PRIORITY> xon <VALUE> kbytes
flow-control buffer llfc xon <VALUE> kbytes
no flow-control buffer priority <PRIORITY> xon <VALUE> kbytes
no flow-control buffer llfc xon <VALUE> kbytes
```

## Description

Allows user configuration of per-priority or LLFC RXTX dynamic XON delta on a physical interface. The **no** form of the command resets the XON delta to the default value.

| Parameter           | Description                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| priority <PRIORITY> | Configures buffer parameters for priority flow control. Range: 0 to 7.                                                                                            |
| llfc                | Configures buffer parameters for link-level flow control.                                                                                                         |
| <VALUE>             | Specifies the offset value below the XOFF limit where XON is asserted and packet transmission resumes. Range: 1 to 40000 kilobytes on 9300/9300S series switches. |

## Examples

Configuring the XON delta of 24 kbytes for PFC priority 4 traffic:

```
switch(config)# interface 1/1/1
```

```
switch(config-if)# flow-control buffer priority 4 xon 24 kbytes
```

Configuring the XON delta of 24 kbytes for LLFC RXTX traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc xon 24 kbytes
```

Resetting the xon delta to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer priority 4 xon 24 kbytes
```

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer llfc xon 24 kbytes
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                            |
|---------|-----------------------------------------|
| 10.11   | Added support for 9300 series switches. |
| 10.10   | Command Introduced.                     |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config-if       | Administrators or local user group members with execution rights for this command. |

## flow-control buffer xoff dynamic

```
flow-control buffer priority <PRIORITY> xoff dynamic <ALPHA>
flow-control buffer llfc xoff dynamic <ALPHA>
no flow-control buffer priority <PRIORITY> xoff dynamic <ALPHA>
no flow-control buffer llfc xoff dynamic <ALPHA>
```

### Description

Allows user configuration of per-priority or LLFC RXTX dynamic XOFF limits on a physical interface. The **no** form of the command resets the threshold to the default value.

| Parameter                              | Description                                                                                                                      |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <code>priority &lt;PRIORITY&gt;</code> | Configures buffer parameters for priority flow control. Range: 0 to 7.                                                           |
| <code>llfc</code>                      | Configures buffer parameters for link-level flow control.                                                                        |
| <code>&lt;ALPHA&gt;</code>             | Specifies the scale factor used to compute the instantaneous buffer limit based on the instantaneous free space. Range: -7 to 3. |

## Examples

Configuring the dynamic XOFF limit of -3 for ingress PFC priority 5 traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 5 xoff dynamic -3
```

Configuring the dynamic XOFF limit of -3 for ingress traffic on an LLFC RXTX port:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc xoff dynamic -3
```

Resetting the xoff dynamic limit to the default:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer priority 5 xoff dynamic
```

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer llfc xoff dynamic
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                            |
|---------|-----------------------------------------|
| 10.11   | Added support for 9300 series switches. |
| 10.10   | Command Introduced.                     |

## Command Information

| Platforms | Command context        | Authority                                                                          |
|-----------|------------------------|------------------------------------------------------------------------------------|
| 9300      | <code>config-if</code> | Administrators or local user group members with execution rights for this command. |

## flow-control buffer xoff static

```
flow-control buffer priority <PRIORITY> xoff static <LIMIT> kbytes
flow-control buffer llfc xoff static <LIMIT> kbytes
no flow-control buffer priority <PRIORITY> xoff static <LIMIT> kbytes
no flow-control buffer llfc xoff static <LIMIT> kbytes
```

## Description

Allows user configuration of per-priority or LLFC RXTX static XOFF limits on a physical interface. The **no** form resets the threshold to the default value.

| Parameter                              | Description                                                                                                                                                                                    |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>priority &lt;PRIORITY&gt;</code> | Configures buffer parameters for priority flow control. Range: 0 to 7.                                                                                                                         |
| <code>llfc</code>                      | Configures buffer parameters for link-level flow control.                                                                                                                                      |
| <code>&lt;LIMIT&gt;</code>             | Specifies the absolute limit programmed for the port or priority. When the in-use amount reaches this limit, the XOFF is asserted. Range: 36 to 40000 kilobytes on 9300/9300S series switches. |

## Examples

Configuring the XOFF static limit of 128 kbytes for PFC priority 6 traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 6 xoff static 128 kbytes
```

Configuring the XOFF static limit of 128 kbytes for LLFC RXTX traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc xoff static 128 kbytes
```

Resetting the xoff static limit to the default:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer priority 6 xoff static
```

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer llfc xoff static
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                            |
|---------|-----------------------------------------|
| 10.11   | Added support for 9300 series switches. |
| 10.10   | Command Introduced.                     |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config-if       | Administrators or local user group members with execution rights for this command. |

## flow-control watchdog

```
flow-control watchdog
no flow-control watchdog
```

### Description

Enables flow control watchdog on a physical interface.

When an excessive amount of lossless traffic stops transmitting, problematic lossless buffer congestion occurs throughout the network. To prevent the situation, egress lossless queues are monitored to detect when no transmissions have occurred for a globally specified detection timeout. When the condition is detected, the flow control watchdog triggers on the affected queue resulting in the following actions:

- The watchdog timeout counter on the interface is incremented.
- All packets occupying the affected queue are discarded.
- New packet arrivals destined for the affected queue are discarded.

After the configured resume interval has elapsed since the trigger, the queue is returned to normal operation.

The **no** form of this command disables flow control watchdog on a physical interface.

---

Flow control watchdog is only supported on interfaces configured with PFC. Link-level flow control is not compatible with flow control watchdog.



When flow control watchdog is enabled, it is active on all lossless queues of the port.

To determine whether the flow control watchdog is enabled on an interface, or to see the number of times the watchdog has been triggered, use the **show interface flow-control** command.

The detection and resume intervals must be configured from the global configuration context.

---

### Examples

Enabling flow control watch on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control watchdog
```

Disabling flow control watch on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control watchdog
```





For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

# flow-control watchdog timeout resume

```
flow-control watchdog timeout <MILLISECONDS> resume <MILLISECONDS>
no flow-control watchdog timeout <MILLISECONDS> resume <MILLISECONDS>
```

## Description

Configures global flow control watchdog parameters, detection time and resume time. The parameters are applied to all interfaces that have flow control watchdog enabled with command **flow-control watchdog**.

The **no** form of this command clears the global configuration parameters for flow control watchdog, restoring timeout and resume time to the platform defaults.

Flow control watchdog must be enabled on specified interfaces.

The configured timing parameters are rounded to what the hardware supports. Use command **show flow control** to show the applied values.

Using fault monitor, an interface can be configured with additional actions such as **notify** or **notify-and-disable** when flow control watchdog triggers exceed the configured threshold. See *Excessive flow control watchdog triggers* in the *Fault monitor* section of the Security Guide (version 10.12 or higher) for your switch model.

| Parameter                                 | Description                                                                                                                                                   |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>timeout &lt;MILLISECONDS&gt;</code> | Specifies the amount of time in milliseconds, that a queue must be paused for watchdog to trigger. Range: 10 to 1500 milliseconds. Default: 100 milliseconds. |
| <code>resume &lt;MILLISECONDS&gt;</code>  | Specifies the duration of time in milliseconds, that a queue remains in the triggered state. Range: 1 to 100000 milliseconds. Default: 100 milliseconds.      |

## Examples

Configuring flow control watchdog global parameters:

```
switch(config) # flow-control watchdog timeout 100 resume 60
```

Removing flow control watchdog global parameters:

```
switch(config) # no flow-control watchdog timeout 100 resume 60
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## interface

```
interface <PORT-NUM>
```

### Description

Switches to the **config-if** context for a physical port. This is where you define the configuration settings for the logical interface associated with the physical port.

| Parameter  | Description                                                         |
|------------|---------------------------------------------------------------------|
| <PORT-NUM> | Specifies a physical port number. Format: <b>member/slot/port</b> . |

### Examples

Configuring an interface:

```
switch(config) # interface 1/1/1
switch(config-if) #
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# interface loopback

```
interface loopback <ID>
no interface loopback <ID>
```

## Description

Creates a loopback interface and changes to the **config-loopback-if** context. Loopback interfaces are layer 3.

The **no** form of this command deletes a loopback interface.

| Parameter  | Description                                          |
|------------|------------------------------------------------------|
| <INSTANCE> | Specifies the loopback interface ID. Range: 1 to 256 |

## Examples

```
switch# config
switch(config)# interface loopback 1
switch(config-loopback-if)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# interface vlan

```
interface vlan <VLAN-ID>
no interface vlan <VLAN-ID>
```

## Description

Creates an interface VLAN also know as an SVI (switched virtual interface) and changes to the **config-if-vlan** context. The specified VLAN must already be defined on the switch.

The **no** form of this command deletes an interface VLAN.

| Parameter | Description                          |
|-----------|--------------------------------------|
| <VLAN-ID> | Specifies the loopback interface ID. |
| none      | Do not reserve any internal VLANs.   |

## Examples

```
switch# config
switch(config)# vlan 10
switch(config-vlan-10)# exit
switch(config)# interface vlan 10
switch(config-if-vlan)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# ip address

```
ip address <IP-ADDR>/<MASK> [secondary]
no ip address <IP-ADDR>/<MASK> [secondary]
```

## Description

Sets an IPv4 address for the current layer 3 interface.

The **no** form of this command removes the IPv4 address from the interface.

| Parameter | Description                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP-ADDR> | Specifies an IP address in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. You can remove leading zeros. For example, the address <b>192.169.005.100</b> becomes <b>192.168.5.100</b> . |
| <MASK>    | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 128.                                                                                           |
| secondary | Specifies a secondary IP address. (Supported on 6300, except for S3L75A, S3L76A, S3L77A.)                                                                                                                                 |

## Examples

Setting the IP address on interface **1/1/1** to **192.168.100.1** with a mask of **24** bits:

```
switch(config)# interface 1/1/1
switch(config-if)# ip address 192.168.100.1/24
```

Removing the IP address **192.168.100.1** with a mask of **24** bits from interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip address 192.168.100.1/24
```

Assigning the IP address **192.168.20.1** with a mask of **24** bits to loopback interface **1**:

```
switch(config)# interface loopback 1
switch(config-loopback-if)# ip address 192.168.20.1/24
```

Assigning the IP address **192.168.199.1** with a mask of **24** bits to interface VLAN **10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# ip address 192.168.199.1/24
```

Removing the IP address **192.168.199.1** with a mask of **24** bits from interface VLAN **10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no ip address 192.168.199.1/24
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                   | Authority                                                                          |
|---------------|---------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if<br>config-loopback-if<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## ip mtu

ip mtu <VALUE>

no ip mtu

### Description

Sets the IP MTU (maximum transmission unit) for an interface. This defines the largest IP packet that can be sent or received by the interface. This value should be less than or equal to the overall MTU for the interface.

The **no** form of this command sets the IP MTU to the default value 1500.

| Parameter | Description                                                      |
|-----------|------------------------------------------------------------------|
| <VALUE>   | Specifies the IP MTU in bytes. Range: 68 to 9198. Default: 1500. |

### Examples

Setting the IP MTU to 576 bytes:

```
switch(config-if)# ip mtu 576
```

Setting the IP MTU to the default value:

```
switch(config-if)# no ip mtu
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release          | Modification                |
|------------------|-----------------------------|
| 10.08            | Subinterface support added. |
| 10.07 or earlier | --                          |

### Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

# ip source-interface

```
ip source-interface {sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-relay |
simplivity | dns | all} {interface <IFNAME> | <IPV4-ADDR>} [vrf <VRF-NAME>]
no ip source-interface {sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-
relay | simplivity | dns | all} [interface <IFNAME> | <IPV4-ADDR>] [vrf <VRF-NAME>]
```

## Description

Sets a single source IP address for a feature on the switch. This ensures that all traffic sent the feature has the same source IP address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.

This command provides two ways to set the source IP addresses: either by specifying a static IP address, or by using the address assigned to a switch interface. If you define both options, then the static IP address takes precedence.

The `no` form of this command deletes the single source IP address for all supported services, or a specific service.

| Parameter                                                                                       | Description                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sflow   tftp   radius   tacacs  <br>ntp   syslog   ubt   dhcp-relay  <br>simplivity   dns   all | Sets a single source IP address for a specific service. The <code>all</code> option sets a global address that applies to all protocols that do not have an address set. For DHCP relay, the address is used as both the source IP and GIADDR.                                                                                       |
| interface <IFNAME>                                                                              | Specifies the name of the interface from which the specified service obtains its source IP address. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.                                                                         |
| <IPV4-ADDR>                                                                                     | Specifies the source IP address to use for the specified service. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the <code>default</code> VRF, if the <code>vrf</code> option is not used). Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. |
| vrf <VRF-NAME>                                                                                  | Specifies the name of a VRF.                                                                                                                                                                                                                                                                                                         |

## Examples

Setting the IPv4 address 10.10.10.5 as the global single source address:

```
switch# config
switch(config)# ip source-interface all 10.10.10.5
```

Setting the secondary IPv4 address 10.10.10.5 on interface 1/1/1 as the global single source address:

```
switch# config
switch(config)# interface 1/1/1
switch(config-if)# ip address 10.10.10.1/24
switch(config-if)# ip address 10.10.10.5/24 secondary
switch(config)# exit
switch(config)# ip source-interface all 10.10.10.5
```

Setting the address 10.10.10.25 on VRF `sflow-vrf` on interface 1/1/2 as the single source address for sFlow:

```
switch(config)# vrf sflow-vrf
switch(config-vrf)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# vrf attach sflow-vrf
switch(config-if)# ip address 10.10.10.25/24
switch(config-if)# exit
switch(config)# ip source-interface sflow interface 1/1/2 vrf sflow-vrf
```

Clearing the global single source IP address **10.10.10.5**:

```
switch(config)# no ip source-interface all 10.10.10.5
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ip tcp mss

```
ip tcp mss <VALUE>
no ip tcp mss <VALUE>
```

### Description

Sets the TCP (Transmission Control Protocol) MSS (Maximum Segment Size) for an interface. When configured, the MSS option in the TCP header is set in the TCP handshake for negotiation during connection establishment. Once the TCP session is established, changing the TCP MSS value on the interface will not affect the existing session.

The **no** form of this command removes the TCP MSS configuration from the interface.



TCP MSS is supported on ROP, SVI, subinterface, and L3 GRE tunnel interface.

| Parameter | Description                                              |
|-----------|----------------------------------------------------------|
| <VALUE>   | Specifies the IPv4 TCP MSS in bytes. Range: 68 to 65495. |

## Examples



Configuring the IPv4 TCP MSS for the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip tcp mss 1460
```

Removing the IPv4 TCP MSS configuration from the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip tcp mss 1460
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification        |
|------------|---------------------|
| 10.14.1000 | Command introduced. |

## Command Information

| Platforms     | Command context                              | Authority                                                                          |
|---------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if<br>config-if-vlan<br>config-gre-if | Administrators or local user group members with execution rights for this command. |

# ip unnumbered

```
ip unnumbered <ifname>
no ip unnumbered <ifname>
```

## Description

The IP unnumbered feature allows the switch to process IP packets without configuring a unique IP address on an interface by telling the router to use the IP address of another selected interface as the address for that link. Once set, this port will borrow the user-configured primary IPv4 address from a lender interface and use that IP address in its L3 control plane exchange.

The **no** version of this command removes IP unnumbered support for this port. Once unset, this port will remove borrowed IPv4 address.

| Parameter | Description           |
|-----------|-----------------------|
| <Ifname > | Name of the interface |

## Usage

The port where IP unnumbered is configured is known as the *borrower* interface. Only route-only ports can borrow an address.

The port the address is borrowed from is known as the *lender* interface. Only a loopback interface can be used as a lender interface. The unnumbered interface and lender interface must belong to the same VRF. Additionally, the lender interface for an IP unnumbered interface cannot itself be configured as unnumbered.

The following caveats apply to this feature:

- Only the primary IPv4 address can be borrowed on an IP unnumbered interface. You cannot configure a secondary IP address for an interface that is already configured as an IP unnumbered interface.
- If an IP address is configured on an interface that is already configured as an IP unnumbered interface, it will function as a normal IP interface.
- An IPv6 unnumbered configuration on the interface is not supported. If **ip unnumbered** is enabled on the interface, only the IPv4 address is borrowed. However, Any IPv6 configurations can co-exist with an ip unnumbered interface.
- An IP unnumbered interface cannot have multiple lender interfaces for the same address family.
- The **ip unnumbered** command requires that the interface borrowing the address is a routed port. The **IP unnumbered** feature is only supported on devices connected with point-to-point interfaces.
- An unnumbered IP address can not be used as tunnel source.
- The unnumbered interface and lender interface must belong to the same VRF.
- Deleting a lender interface removes all the associated IP unnumbered references.

## Examples

Configuring IP unnumbered for a route-only port:

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered loopback1
```

The following examples remove IP unnumbered support for this port. Once unset, this port will remove the borrowed IPv4 address.

```
switch(config)# interface 1/1/1
switch(config-if)# no ip unnumbered loopback1
```

If an IP address is configured on an interface that is already configured as an IP unnumbered interface (or vice versa), both configurations can coexist on the interface. The switch's arbitration logic ensures that static IP configuration is given priority over unnumbered.

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered interface loopback 1
switch(config-if)# ip address 10.16.1.1/24
switch(config-if)# ip address 192.168.1.2/24 secondary

or

switch(config)# interface 1/1/1
switch(config-if)# ip address 10.16.1.1/24
switch(config-if)# ip unnumbered interface loopback 1
switch(config-if)# ip address 192.168.1.2/24 secondary

switch(config)# sh running-config interface
```

```
switch(config-if)# do sh running-config interface 1/1/1
interface 1/1/1
 no shutdown
 ip address 10.16.1.1/24
 ip address 192.168.1.2/24 secondary
 ip unnumbered interface loopback 1
 ! ip unnumbered is ignored when static ip is configured
```

If loopback lender interface does not exist during IP unnumbered configuration, a prompt will be displayed in CLI to allow the user to create that interface.

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered interface loopback 1
Lender port not found.
Do you want to create (y/n)? y
switch(config-if)#

Failure case:
switch(config)# ip unnumbered interface loopback 1
Lender port not found.
Do you want to create (y/n)? y
Lender port: loopback1 creation failed
switch(config-if)
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification       |
|------------|--------------------|
| 10.14.1000 | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## ipv6 address

```
ipv6 address <IPV6-ADDR>/<MASK>{eui64 | [tag <ID>]}
no ipv6 address <IPV6-ADDR>/<MASK>
```

### Description

Sets an IPv6 address on the interface.

The **no** form of this command removes the IPv6 address on the interface.



This command automatically creates an IPv6 link-local address on the interface. However, it does not add the **ipv6 address link-local** command to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the **ipv6 address link-local** command.

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPV6-ADDR> | Specifies the IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where <b>x</b> is a hexadecimal number from 0 to F. You can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address <b>2222:0000:3333:0000:0000:0000:4444:0055</b> becomes <b>2222:0:3333::4444:55</b> . |
| <MASK>      | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 128.                                                                                                                                                                                                                                                                            |
| eui64       | Configure the IPv6 address in the EUI-64 bit format.                                                                                                                                                                                                                                                                                                                                                       |
| tag <ID>    | Configure route tag for connected routes. Range: 0 to 4294967295. Default: 0.                                                                                                                                                                                                                                                                                                                              |

## Examples

Setting the IPv6 address **2001:0db8:85a3::8a2e:0370:7334** with a mask of 24 bits:

```
switch(config-if) # ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
```

Removing the IP address **2001:0db8:85a3::8a2e:0370:7334** with mask of 24 bits:

```
switch(config-if) # no ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

# ipv6 source-interface

```
ipv6 source-interface {sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-relay
| simplivity | dns | all} {interface <IFNAME> | <IPv6-ADDR>} [vrf <VRF-NAME>]
no ipv6 source-interface {sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-
relay | simplivity | dns | all} [interface <IFNAME> | <IPv6-ADDR>] [vrf <VRF-NAME>]
```

## Description

Sets a single source IPv6 address for a feature on the switch. This ensures that all traffic sent the feature has the same source IPv6 address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.

This command provides two ways to set the source IPv6 addresses: either by specifying a static IPv6 address, or by using the address assigned to a switch interface. If you define both options, then the static IPv6 address takes precedence.

The `no` form of this command deletes the single source IPv6 address for all supported protocols, or a specific protocol.

| Parameter                                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sflow   tftp   radius   tacacs  <br>ntp   syslog   ubt   dhcp-relay  <br>simplivity   dns   all | Sets a single source IPv6 address for a specific protocol. The <code>all</code> option sets a global address that applies to all protocols that do not have an address set.                                                                                                                                                                                                  |
| interface <IFNAME>                                                                              | Specifies the name of the interface from which the specified protocol obtains its source IPv6 address.                                                                                                                                                                                                                                                                       |
| <IPv6-ADDR>                                                                                     | Specifies the source IPv6 address to use for the specified protocol. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the <code>default</code> VRF, if the <code>vrf</code> option is not used). Specify the IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. |
| vrf <VRF-NAME>                                                                                  | Specifies the name of the VRF from which the specified protocol sets its source IPv6 address.                                                                                                                                                                                                                                                                                |

## Examples

Configuring the IPv6 address 2001:DB8::1 as the global single source address:

```
switch# config
switch(config)# ipv6 source-interface all 2001:DB8::1/32
```

Configuring the IPv6 address 2001:DB8::1 on VRF `sflow-vrf` on interface 1/1/2 as the single source address for sFlow:

```
switch(config)# vrf sflow-vrf
switch(config-vrf)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# vrf attach sflow-vrf
switch(config-if)# ipv6 address 2001:DB8::1/32
switch(config-if)# exit
switch(config)# ipv6 source-interface sflow interface 1/1/2 vrf sflow-vrf
```

Stop the source IPv6 address from using the IP address on interface **1/1/1** on VRF **one**.

```
switch(config)# no ipv6 source-interface all interface 1/1/1 vrf one
```

Clear the source IPv6 address 2001:DB8::1.

```
switch(config)# no ipv6 source-interface all 2001:DB8::1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ipv6 tcp mss

```
ipv6 tcp mss <VALUE>
no ipv6 tcp mss <VALUE>
```

### Description

Sets the TCP (Transmission Control Protocol) MSS (Maximum Segment Size) for an interface. When configured, the MSS option in the TCP header is set in the TCP handshake for negotiation during connection establishment. Once the TCP session is established, changing the TCP MSS value on the interface will not affect the existing session.

The **no** form of this command removes the TCP MSS configuration from the interface.



TCP MSS is supported on ROP, SVI, subinterface, and L3 GRE tunnel interface.

| Parameter | Description                                              |
|-----------|----------------------------------------------------------|
| <VALUE>   | Specifies the IPv6 TCP MSS in bytes. Range: 68 to 65495. |

## Examples

Configuring the IPv6 TCP MSS for the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 tcp mss 1440
```

Removing the IPv6 TCP MSS configuration from the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 tcp mss 1440
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification        |
|------------|---------------------|
| 10.14.1000 | Command introduced. |

## Command Information

| Platforms     | Command context                              | Authority                                                                          |
|---------------|----------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-if<br>config-if-vlan<br>config-gre-if | Administrators or local user group members with execution rights for this command. |

## l3-counters

```
l3-counters [rx | tx]
no l3-counters [rx | tx]
```

### Description

Enables counters on a layer 3 interface. By default, all interfaces are layer 3. To change a layer 2 interface to layer 3, use the **routing** command.

The **no** form of this command, with no specification, disables both transmit and receive counters on a layer 3 interface. To disable transmit (**tx**) or receive (**rx**) counters only, specify the counter type you want to disable.

| Parameter | Description                  |
|-----------|------------------------------|
| rx        | Specifies receive counters.  |
| tx        | Specifies transmit counters. |

## Examples

Enabling layer 3 transmit counters on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# 13-counters tx
```

Disabling layer 3 transmit and receive counters on interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no 13-counters
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                   |
|------------------|------------------------------------------------|
| 10.08            | Added support for 13 counters on subinterfaces |
| 10.07 or earlier | --                                             |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## mtu

```
mtu <VALUE>
no mtu
```

## Description

Sets the MTU (maximum transmission unit) for an interface. This defines the maximum size of a layer 2 (Ethernet) frame. Frames larger than the MTU (1500 bytes by default) are dropped and cause an ICMP fragmentation-needed message to be sent back to the originator.

To support jumbo frames (frames larger than 1522 bytes), increase the MTU as required by your network. A frame size of up to 9198 bytes is supported.

The largest possible layer 1 frame will be 18 bytes larger than the MTU value to allow for link layer headers and trailers.

The **no** form of this command sets the MTU to the default value 1500.

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| <VALUE>   | Specifies the MTU in bytes. Range: 46 to 9198. Default: 1500. |

## Examples

Setting the MTU on interface **1/1/1** to 1000 bytes:



```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# mtu 1000
```

Setting the MTU on interface **1/1/1** to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# no mtu
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## persona

```
persona {access | uplink | custom <PERSONA-NAME>} [copy | attach]
no persona {access | uplink | custom <PERSONA-NAME>} [copy | attach]
```

## Description

Associates one of three persona types with an interface to classify the purpose or role of an interface. On the 10000 Switch Series, “access” persona ports are typically connected to workloads / VMs, and the “uplink” (fabric) persona ports are connected to the core / spine.

The **no** form of this command removes the interface persona.

| Parameter             | Description                                                                                                                  |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------|
| access                | Selects the <b>access</b> persona type.                                                                                      |
| uplink                | Selects the <b>uplink</b> persona type.                                                                                      |
| custom <PERSONA-NAME> | Selects the <b>custom</b> persona type with a user-provided name. Range: 1 to 64 printable ASCII characters including space. |
| copy                  | Specifies the mode: copies settings from the persona interface of the same name.                                             |

| Parameter           | Description                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------|
| <code>attach</code> | Specifies the mode: attaches the specified interface to the persona interface of the same name. |

## Usage

- If the mode is specified, either `copy` or `attach`, the interface configuration is dependent on the interface template whose name is "access", "uplink", or "<PERSONA-NAME>". On the other hand, if the mode is not specified, then the persona is just a label in the interface, and its configuration is not modified even if the interface persona exists. When configuring the mode, one of the following options is possible:
  - The **copy** option performs a one-time copy of the template interface. Subsequent changes to the template are not copied and the 'persona' setting is just a label. If the mode is set to **copy** and the interface persona does not exist, then the CLI command fails with the message "Interface persona not found".
  - The **attach** option performs a copy of the template interface, and subsequent changes to the template interface configuration are immediately applied to all attached interfaces. The template interface does not need to exist before attaching other interfaces to it. After attaching a template, the copied settings can be modified for an individual interface. However, any change in the attached template will overwrite the modified values with the new template values.
- When a mode is specified, it should match an interface created with the command `interface persona <PERSONA-NAME>`. The only exception to this rule is when the mode is set to `attach` and the persona does not already exist.
- The mode is only available to be configured for an interface that meets the following conditions:
  - IS a physical interface
  - IS NOT a LAG member
  - IS NOT a persona interface

## Examples

Configuring an access persona:

```
switch(config)# interface 1/1/1
switch(config-if)# persona access
```

Configuring an uplink persona:

```
switch(config)# interface 1/1/1
switch(config-if)# persona uplink
```

Configuring a custom persona named "mypersona":

```
switch(config)# interface 1/1/1
switch(config-if)# persona custom mypersona
```

Removing the persona setting.

```
switch(config-if)# no persona
```

Copying a predefined persona name configuration to an interface:

1. Configuring the interface persona:

```
switch(config)# interface persona uplink
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# vlan access 100
switch(config-if)# exit
```

2. Applying the configuration from the persona named "mypersona" with **copy** mode:

```
switch(config)# interface 1/1/1
switch(config-if)# persona custom mypersona copy
switch(config-if)# exit
```

Attaching a custom persona name named "mypersona" to several interfaces simultaneously:

1. Configuring an interface persona named "mypersona":

```
switch(config)# interface persona mypersona
switch(config-if)# no shutdown
switch(config-if)# vrf attach upstream
switch(config-if)# exit
```

2. Applying the "mypersona" configuration with **attach** mode:

```
switch(config)# interface 1/1/1-1/1/24
switch(config-if)# persona custom mypersona attach
switch(config-if)# exit
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification                                                                       |
|------------|------------------------------------------------------------------------------------|
| 10.16.1000 | Introduced support for AAA and Port-access configurations on the persona interface |
| 10.10      | Added optional parameters: attach, copy.                                           |
| 10.09      | Command introduced.                                                                |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## rate-interval

```
rate-interval <VALUE>
no rate-interval
```

### Description

This command sets the time interval to calculate interface rates. Lower intervals are more useful for detecting traffic bursts, but may increase computation load to the overall system. Intervals must be a multiple of five seconds. The command-line interface will not accept a rate interval value that is not a multiple of five.

The **no** form of this command sets the rate collection interval to the default value of 300 seconds.

| Parameter | Description                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <VALUE>   | The statistics rate collection interval in seconds. The supported range is 5-300 seconds, where the number of seconds is a multiple of five. |

### Examples

Setting the rate collection interval to 50 seconds

```
switch(config)# interface 1/1/1
switch(config-if)# rate-interval 50
```

Setting the rate collection interval to the default value:

```
switch(config-if)# no rate-interval
```

The following example shows the command-line interface warning that appears while configuring an invalid rate-interval.

```
switch(config)# interface 1/1/1
switch(config-if)# rate interval 6
The interval must be a multiple of 5.
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Usage

The rate collection interval must be configured in the multiples of 5. Any other value will be rejected and the CLI will display the error message, **The interval must be a multiple of 5.**

### Command History

| Release    | Modification                                       |
|------------|----------------------------------------------------|
| 10.12.1000 | Command supported on all platforms.                |
| 10.12      | Command Introduced on 6300 and 8360 Switch series. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## routing

routing  
no routing

### Description

Enables routing support on an interface, creating a L3 (layer 3) interface on which the switch can route IPv4/IPv6 traffic to other devices.

By default, routing is enabled on all interfaces.

The **no** form of this command disables routing support on an interface, creating a L2 (layer 2) interface.



If you enable this configuration, collection of flow tracking statistics is disabled.

### Examples

Enabling routing support on an interface:

```
switch(config-if) # routing
```

Disabling routing support on an interface:

```
switch(config-if) # no routing
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## show allow-unsupported-transceiver

show allow-unsupported-transceiver

### Description

Displays configuration and status of unsupported transceivers.

### Examples

Showing unallowed unsupported transceivers:

```
switch(config)# show allow-unsupported-transceiver
Allow unsupported transceivers : no
Logging interval : 1440 minutes

Port Type Status

1/1/31 SFP-SX unsupported
1/1/32 SFP-1G-BXD unsupported
1/1/2 SFP28DAC3 unsupported
```

Showing allowed unsupported transceivers:

```
switch# show allow-unsupported-transceiver
Allow unsupported transceivers : yes
Logging interval : 1440 minutes

Port Type Status

1/1/31 SFP-SX unsupported-allowed
1/1/32 SFP-1G-BXD unsupported-allowed
1/1/2 SFP28DAC3 unsupported
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

# show interface

```
show interface [<IFNNAME>|<IFRANGE>] [brief | physical]
show interface [<IFNNAME>|<IFRANGE>] [extended [non-zero] | [human-readable]]
show interface [<IFNNAME>] monitor [human-readable]
show interface [lag | loopback | tunnel | vlan] [<ID>] [brief]
show interface lag [<LAG-ID>] [extended [non-zero] | [human-readable]]
show interface lag [<LAG-ID>] monitor [human-readable]
show interface vxlan <VXLAN-ID> [brief | physical]
show interface vxlan <VXLAN-ID> [brief | physical]
```

## Description

Shows active configurations and operational status information for interfaces.

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IFNAME>       | Specifies a interface name.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <IFRANGE>      | Specifies the port identifier range.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| brief          | Shows brief info in tabular format.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| physical       | Shows the physical connection info in tabular format.                                                                                                                                                                                                                                                                                                                                                                                                              |
| extended       | Shows additional statistics, including the <b>tx filtered</b> and <b>rx filtered</b> counters. <ul style="list-style-type: none"><li>▪ Rx filter packets are protocol packets received when the protocol is disabled on the switch and there is only one port in the VLAN. Protocols include OSPF, PIM, RIP, LACP, and LLDP.</li><li>▪ An example of a Tx filtered packet would be a multicast packet being filtered from going out of the ingress port.</li></ul> |
| human-readable | Shows statistics rounded to the nearest power of 1000, for example, 1K, 345M, 2G. This is available only in the CLI interface output.                                                                                                                                                                                                                                                                                                                              |
| non-zero       | Shows only non zero statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| LAG            | Shows LAG interface information.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| monitor        | Continuously monitor interface statistics.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| LOOPBACK       | Shows loopback interface information.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| TUNNEL         | Shows tunnel interface information.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| VLAN           | Shows VLAN interface information.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <LAG-ID>       | Specifies the LAG number. Range: 1-256                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <LOOPBACK-ID>  | Specifies the LOOPBACK number. Range: 0-255                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <TUNNEL-ID>    | Specifies the tunnel ID. Range: 1-255                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <VLAN-ID>      | Specifies the VLAN ID. Range: 1-4094                                                                                                                                                                                                                                                                                                                                                                                                                               |
| VXLAN          | Shows the VXLAN interface information.                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Parameter  | Description                                          |
|------------|------------------------------------------------------|
| <VXLAN-ID> | Specifies the VXLAN interface identifier. Default: 1 |

## Examples

Showing interface information when it is configured as a route-only port:

```
switch# show interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Link state: up for 2 days (since Sun Jun 21 05:30:22 UTC 2020)
Link transitions: 1
Description: backup data center link
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 1500
Type 1GbT
Full-duplex
qos trust none
Speed 1000 Mb/s
Auto-negotiation is on
Flow-control: off
Error-control: off
L3 Counters: Rx Enabled, Tx Enabled
Rate collection interval: 300 seconds
```

| Rates         | RX   | TX   | Total (RX+TX) |
|---------------|------|------|---------------|
| Mbits / sec   | 0.00 | 0.00 | 0.00          |
| KPkts / sec   | 0.00 | 0.00 | 0.00          |
| Unicast       | 0.00 | 0.00 | 0.00          |
| Multicast     | 0.00 | 0.00 | 0.00          |
| Broadcast     | 0.00 | 0.00 | 0.00          |
| Utilization % | 0.00 | 0.00 | 0.00          |

| Statistics   | RX  | TX  | Total |
|--------------|-----|-----|-------|
| Packets      | 0   | 0   | 0     |
| Unicast      | 0   | 0   | 0     |
| Multicast    | 0   | 0   | 0     |
| Broadcast    | 0   | 0   | 0     |
| Bytes        | 0   | 0   | 0     |
| Jumbos       | 0   | 0   | 0     |
| Dropped      | 0   | 0   | 0     |
| Filtered     | 0   | 0   | 0     |
| Pause Frames | 0   | 0   | 0     |
| L3 Packets   | 0   | 0   | 0     |
| L3 Bytes     | 0   | 0   | 0     |
| Errors       | 0   | 0   | 0     |
| CRC/FCS      | 0   | n/a | 0     |
| Collision    | n/a | 0   | 0     |
| Runts        | 0   | n/a | 0     |
| Giants       | 0   | n/a | 0     |
| Other        | 0   | 0   | 0     |

Showing information when the interface is currently linked at a downshifted speed:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
```



```
...
Auto-negotiation is on with downshift active
```

Showing information when the interface is shut down during a VSX split:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is down
Admin state is up
State information: Disabled by VSX
Link state: down for 3 days (since Tue Mar 16 05:20:47 UTC 2021)
Link transitions: 0
Description:
Hardware: Ethernet, MAC Address: 04:09:73:62:90:e7
MTU 1500
Type SFP+DAC3
Full-duplex
qos trust none
Speed 0 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: 1502-1505
Rate collection interval: 300 seconds
```

| Rate        | RX   | TX   | Total (RX+TX) |
|-------------|------|------|---------------|
| Mbits / sec | 0.00 | 0.00 | 0.00          |
| KPkts / sec | 0.00 | 0.00 | 0.00          |
| Unicast     | 0.00 | 0.00 | 0.00          |
| Multicast   | 0.00 | 0.00 | 0.00          |
| Broadcast   | 0.00 | 0.00 | 0.00          |
| Utilization | 0.00 | 0.00 | 0.00          |

| Statistic    | RX  | TX  | Total |
|--------------|-----|-----|-------|
| Packets      | 0   | 0   | 0     |
| Unicast      | 0   | 0   | 0     |
| Multicast    | 0   | 0   | 0     |
| Broadcast    | 0   | 0   | 0     |
| Bytes        | 0   | 0   | 0     |
| Jumbos       | 0   | 0   | 0     |
| Dropped      | 0   | 0   | 0     |
| Pause Frames | 0   | 0   | 0     |
| Errors       | 0   | 0   | 0     |
| CRC/FCS      | 0   | n/a | 0     |
| Collision    | n/a | 0   | 0     |
| Runts        | 0   | n/a | 0     |
| Giants       | 0   | n/a | 0     |

Showing the monitor information:



In monitor mode, the CLI refreshes data automatically until it is exited by entering **q**. Pressing **?** opens the help menu to display which options are available in this context.

```
Interface 1/1/1 is up
```

| Rate             | RX           | TX           | Total (RX+TX) |
|------------------|--------------|--------------|---------------|
| -----            | -----        | -----        | -----         |
| MBits / sec      | 30196.43     | 30196.43     | 60392.85      |
| MPkts / sec      | 58977.39     | 58977.40     | 117954.79     |
| Unicast          | 0.00         | 0.00         | 0.00          |
| Multicast        | 58977.39     | 58977.40     | 117954.79     |
| Broadcast        | 0.00         | 0.00         | 0.00          |
| Utilization %    | 75.49        | 75.49        | 150.98        |
| Statistic        | RX           | TX           | Total (RX+TX) |
| -----            | -----        | -----        | -----         |
| Packets          | 4756527649   | 4756527865   | 9513055514    |
| Unicast          | 0            | 0            | 0             |
| Multicast        | 4756527649   | 4756527865   | 9513055514    |
| Broadcast        | 2            | 0            | 2             |
| Bytes            | 304417778668 | 304417795428 | 608835574096  |
| Jumbos           | 0            | 0            | 0             |
| Dropped          | 0            | 19028847730  | 19028847730   |
| Pause Frames     | 0            | 0            | 0             |
| Errors           | 0            | 0            | 0             |
| CRC/FCS          | 0            | n/a          | 0             |
| help: ?, quit: q |              |              |               |

```

Help for Interface Monitor
h Toggle human-readable mode
c Clear interface statistics
Does not apply to rates
Arrows, PgUp, PgDn, Home, End
Navigate interface statistics
Delay: 2
help: ?, quit: q

```

Showing the output for interface 1/1/1 in human-readable format:



In human-readable format, the **< 1** symbol for **Utilization** indicates that the amount of packets is between zero and one. This is true in cases where the number of bytes increases but the number of packets and the **Utilization** value is not displayed even in the normal output, where the human-readable parameter is not included in the command.

```

switch(config-if)# show interface 1/1/1 human-readable
Interface 1/1/1 is up
Rate
```

|               | RX    | TX    | Total (RX+TX) |
|---------------|-------|-------|---------------|
| -----         | ----- | ----- | -----         |
| Bits / sec    | 3M    | 3M    | 6M            |
| Pkts / sec    | 316   | 316   | 633           |
| Unicast       | 319   | 319   | 638           |
| Multicast     | 0     | 0     | 0             |
| Broadcast     | 0     | 0     | 0             |
| Utilization % | < 1   | < 1   | < 1           |
| Statistic     | RX    | TX    | Total         |
| -----         | ----- | ----- | -----         |
| Packets       | 577K  | 577K  | 1M            |
| Unicast       | 577K  | 577K  | 1M            |
| Multicast     | 0     | 51    | 51            |
| Broadcast     | 0     | 15    | 15            |
| Bytes         | 744M  | 745M  | 1G            |
| Jumbos        | 0     | 0     | 0             |
| Dropped       | 0     | 0     | 0             |

|              |     |     |   |
|--------------|-----|-----|---|
| Filtered     | 0   | 0   | 0 |
| Pause Frames | 0   | 0   | 0 |
| Errors       | 0   | 0   | 0 |
| CRC/FCS      | 0   | n/a | 0 |
| Collision    | n/a | 0   | 0 |
| Runts        | 0   | n/a | 0 |
| Giants       | 0   | n/a | 0 |

Showing information about extended counters:



The output of the `show interface extended` command varies depending on the switch model and configuration.

```
switch(config-if)# show interface 1/1/17 extended

Interface 1/1/17

Statistics Value

Dot1d Tp Port In Frames 547
Dot1d Tp Port Out Frames 608
Dot3 In Pause Frames 0
Dot3 Out Pause Frames 0
Ethernet Stats Broadcast Packets 19
Ethernet Stats Bytes 40162
Ethernet Stats Packets 342
...

Error-Statistics Value

Dot1d Base Port MTU Exceeded Discards 0
Dot3 Control In Unknown Opcodes 0
Dot3 Stats Alignment Errors 0
Dot3 Stats FCS Errors 0
Dot3 Stats Frame Too Longs 0
Dot3 Stats Internal Mac Transmit Errors 0
Ethernet RX Oversize Packets 0
...
```

Showing interface link-status:

```
switch# show interface link-status

Port Type Physical Link Last
 Type Link State Transitions Change

1/1/1 1G-BT down 0 --
1/1/2 1G-BT up 1 1 minute ago (Fri Mar 09
12:36:56 UTC 2018)
1/1/3 1G-BT up 1 1 minute ago (Fri Mar 09
12:36:56 UTC 2018)
1/1/4 -- down 0 --
1/1/5 -- down 0 --
```

Showing interface loopback 1 link-status:

```

Port Type Physical Link Last
Link State Transitions Change

loopback1 -- up -- --

```

Showing interface 1/1/2-1/1/3 link-status:

```

Port Type Physical Link Last
Link State Transitions Change

1/1/2 1G-BT up 1 1 minute ago (Fri Mar 09
12:36:56 UTC 2018)
1/1/3 1G-BT up 1 1 minute ago (Fri Mar 09
12:36:56 UTC 2018)

```

Showing interface link-status:

```

switch# show interface link-status

Port Type Physical Link Link Flaps Last
Link State Transitions Ignored Change

1/1/1 1G-BT down 0 0 --
1/1/2 1G-BT up 1 0 1 minute ago
(Fri Mar 09 12:36:56 UTC 2018)
1/1/3 1G-BT up 1 0 1 minute ago
(Fri Mar 09 12:36:56 UTC 2018)
1/1/4 -- down 0 0 --
1/1/5 -- down 0 0 --

```

Showing state information when interface is blocked:

```

8360(config-if)# show interface 1/1/1

Interface 1/1/1 is up (Blocked)
Admin state is up
State information: Blocked by UDLD
Link state: up for 1 minute (since Mon Jun 10 09:25:27 UTC 2024)
Link transitions: 1
Description:
Persona:
Hardware: Ethernet, MAC Address: 00:fd:45:67:85:91
MTU 1500
Type 10G-LR / 10G SFP+ LR
Full-duplex
qos trust none
Speed 10000 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: access
Access VLAN: 1
Rate collection interval: 300 seconds

Rate RX TX Total (RX+TX)

```

|               |      |      |       |
|---------------|------|------|-------|
| Mbits / sec   | 0.00 | 0.00 | 0.00  |
| KPkts / sec   | 0.00 | 0.00 | 0.00  |
| Unicast       | 0.00 | 0.00 | 0.00  |
| Multicast     | 0.00 | 0.00 | 0.00  |
| Broadcast     | 0.00 | 0.00 | 0.00  |
| Utilization % | 0.00 | 0.00 | 0.00  |
| Statistic     | RX   | TX   | Total |
| Packets       | 15   | 15   | 30    |
| Unicast       | 12   | 12   | 24    |
| Multicast     | 3    | 3    | 6     |
| Broadcast     | 0    | 0    | 0     |
| Bytes         | 1350 | 1350 | 2700  |
| Jumbos        | 0    | 0    | 0     |
| Dropped       | 0    | 0    | 0     |
| Pause Frames  | 0    | 0    | 0     |
| Errors        | 0    | 0    | 0     |
| CRC/FCS       | 0    | n/a  | 0     |
| Collision     | n/a  | 0    | 0     |
| Runts         | 0    | n/a  | 0     |
| Giants        | 0    | n/a  | 0     |



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

## Command History

| Release          | Modification                                            |
|------------------|---------------------------------------------------------|
| 10.15            | Added state information when port goes into down state. |
| 10.11            | Added <code>monitor</code> parameter.                   |
| 10.10            | Added <code>human-readable</code> parameter.            |
| 10.07 or earlier | --                                                      |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show interface dom

```
show interface [<INTERFACE-ID>] dom [detail] [vsx-peer]
```

### Description

Shows diagnostics information and alarm/warning flags for the optical transceivers (SFP, SFP+, QSFP+). This information is known as DOM (Digital Optical Monitoring). DOM information also consists of vendor determined thresholds which trigger high/low alarms and warning flags.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-ID> | Specifies an interface. Format: <b>member/slot/port</b> .                                                                                                                                                                        |
| detail         | Show detailed information.                                                                                                                                                                                                       |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

```
switch# show interface dom
```

| Port  | Type     | Channel | Temperature<br>(Celsius) | Voltage<br>(Volts) | Tx Bias<br>(mA) | Rx Power<br>(mW/dBm) | Tx Power<br>(mW/dBm) |
|-------|----------|---------|--------------------------|--------------------|-----------------|----------------------|----------------------|
| 1/1/1 | SFP+SR   |         | 47.65                    | 3.31               | 8.40            | 0.08, -10.96         | 0.63, -2.49          |
| 1/1/2 | SFP+SR   |         | n/a                      | n/a                | n/a             | n/a                  | n/a                  |
| 1/1/3 | SFP+DA3  |         | 42.10                    | 3.24               | n/a             | n/a                  | n/a                  |
| 1/1/4 | QSFP+SR4 | 1       | 44.46                    | 3.30               | 6.12            | 0.08, -10.96         | 0.63, -1.95          |
| 2     |          |         | 44.46                    | 3.30               | 6.04            | 0.08, -10.96         | 0.63, -2.00          |
| 3     |          |         | 44.46                    | 3.30               | 6.51            | 0.08, -10.96         | 0.60, -2.16          |
| 4     |          |         | 44.46                    | 3.30               | 6.19            | 0.08, -10.96         | 0.63, -1.94          |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show interface flow-control

```
show interface [<IFNNAME>|<IFRANGE>] flow-control [detail]
```

## Description

Shows the flow control configuration, status, and statistics of the specified interface for interfaces on which flow control is enabled.



If **detail** is not specified, this command shows a summary of all flow controlled interfaces with one interface per line. If **detail** is specified, this command shows flow control detailed statistics.



As of AOS-CX 10.10, the separate **show flow-control** command has been removed, with it being effectively replaced by this command.

| Parameter          | Description                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IFNAME> <IFRANGE> | Specifies the interface (port) name or range. When no interface range is specified, only interfaces with flow control enabled in the configuration or status are shown. |
| detail             | Shows detailed information.                                                                                                                                             |

## Examples

Showing summary flow control information:

```
switch# show interface flow-control

Port Flow
 Control

1/1/1 config: llfc rx
 status: llfc rx
1/1/2 config: llfc rx
 status: none
```

Showing summary flow control information with PFC:

```
switch# show interface flow-control

Port Flow
 Control

1/1/1 config: pfc rxtx-1,2
 status: pfc rxtx-1,2
1/1/2 config: pfc rxtx-5
 status: none
```

Showing summary flow control information with PFC:

```
switch# show interface flow-control
 Flow Control Watchdog Settings
 Trigger Timeout: 100 milliseconds
 Resume Time: 100 milliseconds

Port Flow Watchdog Watchdog
 Control Status Timeouts

1/1/1 config: llfc rx
 status: llfc rx
1/1/2 config: llfc rx incompatible 0
```

```

status: llfc rx
1/1/10 config: pfc rxtx-1,2 enabled 1234
 status: pfc rxtx-1,2
1/1/12 config: pfc rxtx-1,2 error 0
 status: pfc rxtx-1,2
1/1/32:4 config: pfc rxtx-5
 status: pfc rxtx-5

```

Showing summary flow control information where the configuration does not match status due to a reboot required to apply PFC configuration in hardware:

```

switch# show interface flow-control

Flow Control Watchdog Settings
 Trigger Timeout: 100 milliseconds (actual: not applied)
 Resume Time: 100 milliseconds (actual: not applied)

Port Flow Control Watchdog Status Watchdog

1/1/1 config: llfc rx status: llfc rx
1/1/2 config: llfc rx status: llfc rx incompatible 0
1/1/10 config: pfc rxtx-1,2 status: none pending 1234
1/1/12 config: pfc rxtx-1,2 status: none pending 0
1/1/32:4 config: pfc rxtx-5 status: none

```

Showing detailed flow control information with RX flow control enabled:

```

switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rx

Statistics RX

Dot3 Pause Frames 0

```

Showing detailed flow control information with RX flow control enabled:

```

switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rx
Flow-control watchdog: disabled

```



| Statistics        | RX    |
|-------------------|-------|
| -----             | ----- |
| Dot3 Pause Frames | 0     |

Showing detailed flow control information with RXTX flow control enabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rxtx
```

| Statistics        | RX    | TX    |
|-------------------|-------|-------|
| -----             | ----- | ----- |
| Dot3 Pause Frames | 0     | 0     |

Showing detailed flow control information with PFC enabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
```

| Statistics         | RX    | TX    |
|--------------------|-------|-------|
| -----              | ----- | ----- |
| Priority 0 Pauses  | 0     | 0     |
| Priority 1 Pauses  | 0     | 0     |
| Priority 2 Pauses  | 0     | 0     |
| Priority 3 Pauses  | 0     | 0     |
| Priority 4 Pauses  | 0     | 0     |
| Priority 5 Pauses  | 0     | 0     |
| Priority 6 Pauses  | 0     | 0     |
| Priority 7 Pauses  | 0     | 0     |
| Total Pause Frames | 0     | 0     |

Showing detailed flow control information with PFC enabled and flow control watchdog disabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
Flow-control watchdog: disabled
```

| Statistics        | RX    | TX    |
|-------------------|-------|-------|
| -----             | ----- | ----- |
| Priority 0 Pauses | 0     | 0     |
| Priority 1 Pauses | 0     | 0     |
| Priority 2 Pauses | 0     | 0     |
| Priority 3 Pauses | 0     | 0     |
| Priority 4 Pauses | 0     | 0     |

```

Priority 5 Pauses 0 0
Priority 6 Pauses 0 0
Priority 7 Pauses 0 0
Total Pause Frames 0 0
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
Flow-control watchdog: disabled

```

| Statistics         | RX | TX |
|--------------------|----|----|
| Priority 0 Pauses  | 0  | 0  |
| Priority 1 Pauses  | 0  | 0  |
| Priority 2 Pauses  | 0  | 0  |
| Priority 3 Pauses  | 0  | 0  |
| Priority 4 Pauses  | 0  | 0  |
| Priority 5 Pauses  | 0  | 0  |
| Priority 6 Pauses  | 0  | 0  |
| Priority 7 Pauses  | 0  | 0  |
| Total Pause Frames | 0  | 0  |

Showing detailed flow control information with both PFC and flow control watchdog enabled:

```

switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
Flow-control watchdog: enabled

```

| Statistics         | RX | TX |
|--------------------|----|----|
| Priority 0 Pauses  | 0  | 0  |
| Priority 1 Pauses  | 0  | 0  |
| Priority 2 Pauses  | 0  | 0  |
| Priority 3 Pauses  | 0  | 0  |
| Priority 4 Pauses  | 0  | 0  |
| Priority 5 Pauses  | 0  | 0  |
| Priority 6 Pauses  | 0  | 0  |
| Priority 7 Pauses  | 0  | 0  |
| Total Pause Frames | 0  | 0  |

| Queue   | Watchdog Timeouts |
|---------|-------------------|
| Queue 0 | 0                 |
| Queue 1 | 0                 |
| Queue 2 | 0                 |
| Queue 3 | 0                 |
| Queue 4 | 0                 |
| Queue 5 | 0                 |
| Queue 6 | 0                 |
| Queue 7 | 0                 |

Showing detailed flow control information when flow control watchdog is enabled in the configuration but it could not be applied because the configured flow control mode is not compatible with watchdog:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rx
Flow-control watchdog: incompatible
```

Showing detailed flow control information when flow control watchdog is enabled in the configuration but could not be applied because a compatible flow control mode first requires a reboot:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: off
Flow-control watchdog: pending
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                                           |
|---------|--------------------------------------------------------|
| 10.10   | Examples updated with new and changed output elements. |
| 10.08   | Command introduced.                                    |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show interface link-diagnostics

```
show interface [<IFNAME>|<IFRANGE>] link-diagnostics
```

### Description

Shows information about select link diagnostics, including MAC, PHY, and Transceiver diagnostics.

| Parameter        | Description                          |
|------------------|--------------------------------------|
| <IFNAME>         | Specifies a interface name.          |
| <IFRANGE>        | Specifies the port identifier range. |
| link-diagnostics | Shows link diagnostics information.  |

## Examples

Showing interface information for 1/1/12 link diagnostics:

```
switch# show interface 1/1/12 link-diagnostics
```

| Interface 1/1/12               | Current State    | Changes | Last Change    |
|--------------------------------|------------------|---------|----------------|
| Port Status                    | Waiting for link |         |                |
| Link Down Reason               | Local fault      |         |                |
| Transceiver                    |                  |         |                |
| No transceiver                 | --               | 0       | --             |
| TX Fault                       | --               | 0       | --             |
| Transceiver error              | --               | 0       | --             |
| System error                   | --               | 0       | --             |
| DOM error                      | --               | 0       | --             |
| Configuring transceiver        | --               | 0       | --             |
| Transceiver disabled           | --               | 0       | --             |
| Transceiver unsupported        | --               | 0       | --             |
| MAC and PHY                    |                  |         |                |
| TX Disabled                    | --               | 0       | --             |
| Autoneg Incomplete             | --               | 0       | --             |
| No Signal Detected             | --               | 0       | --             |
| No RX Lock                     | True             | 1       | 22 seconds ago |
| (Tue Nov 14 14:30:48 UTC 2023) |                  |         |                |
| Remote Fault                   | --               | 0       | --             |
| Local Fault                    | True             | 1       | 22 seconds ago |
| (Tue Nov 14 14:30:48 UTC 2023) |                  |         |                |
| Link State                     | Down             | 1       | 16 seconds ago |
| (Tue Nov 14 14:30:54 UTC 2023) |                  |         |                |

```
switch# show interface 1/1/12 link-diagnostics
```

| Interface 1/1/12                   | Current State | Changes | Last Change |
|------------------------------------|---------------|---------|-------------|
| Port Status                        | Link up       |         |             |
| Link Down Reason                   | --            |         |             |
| Transceiver                        |               |         |             |
| No transceiver                     | --            | 0       | --          |
| TX Fault                           | --            | 0       | --          |
| Transceiver error                  | --            | 0       | --          |
| System error                       | --            | 0       | --          |
| DOM error                          | --            | 0       | --          |
| Configuring transceiver            | --            | 0       | --          |
| Transceiver disabled               | --            | 0       | --          |
| Transceiver unsupported            | --            | 0       | --          |
| MAC and PHY                        |               |         |             |
| TX Disabled                        | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| Autoneg Incomplete                 | --            | 0       | --          |
| No Signal Detected                 | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| No RX Lock                         | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| Remote Fault                       | --            | 2       | 21 seconds  |
| ago (Tue Nov 14 14:30:49 UTC 2023) |               |         |             |
| Local Fault                        | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| Link State                         | Up            | 1       | 16 seconds  |
| ago (Tue Nov 14 14:30:54 UTC 2023) |               |         |             |

Showing interface information for 1/1/7-1/1/8 link-diagnostics:

```
switch# show interface 1/1/7-1/1/8 link-diagnostics
```

| Interface 1/1/7                    | Current State | Changes | Last Change |
|------------------------------------|---------------|---------|-------------|
| Port Status                        | Link up       |         |             |
| Link Down Reason                   | --            |         |             |
| Transceiver                        |               |         |             |
| No transceiver                     | --            | 0       | --          |
| TX Fault                           | --            | 0       | --          |
| Transceiver error                  | --            | 0       | --          |
| System error                       | --            | 0       | --          |
| DOM error                          | --            | 0       | --          |
| Configuring transceiver            | --            | 0       | --          |
| Transceiver disabled               | --            | 0       | --          |
| Transceiver unsupported            | --            | 0       | --          |
| MAC and PHY                        |               |         |             |
| TX Disabled                        | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| Autoneg Incomplete                 | --            | 0       | --          |
| No Signal Detected                 | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| No RX Lock                         | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| Remote Fault                       | --            | 2       | 21 seconds  |
| ago (Tue Nov 14 14:30:49 UTC 2023) |               |         |             |
| Local Fault                        | --            | 2       | 22 seconds  |
| ago (Tue Nov 14 14:30:48 UTC 2023) |               |         |             |
| Link State                         | Up            | 1       | 16 seconds  |
| ago (Tue Nov 14 14:30:54 UTC 2023) |               |         |             |

| Interface 1/1/8                | Current State | Changes | Last Change    |
|--------------------------------|---------------|---------|----------------|
| Port Status                    | Link up       |         |                |
| Link Down Reason               | --            |         |                |
| Transceiver                    |               |         |                |
| No transceiver                 | --            | 0       | --             |
| TX Fault                       | --            | 0       | --             |
| Transceiver error              | --            | 0       | --             |
| System error                   | --            | 0       | --             |
| DOM error                      | --            | 0       | --             |
| Configuring transceiver        | --            | 0       | --             |
| Transceiver disabled           | --            | 0       | --             |
| Transceiver unsupported        | --            | 0       | --             |
| MAC and PHY                    |               |         |                |
| TX Disabled                    | --            | 2       | 22 seconds ago |
| (Tue Nov 14 14:30:48 UTC 2023) |               |         |                |
| Autoneg Incomplete             | --            | 0       | --             |
| No Signal Detected             | --            | 2       | 22 seconds ago |
| (Tue Nov 14 14:30:48 UTC 2023) |               |         |                |
| No RX Lock                     | --            | 2       | 22 seconds ago |
| (Tue Nov 14 14:30:48 UTC 2023) |               |         |                |
| Remote Fault                   | --            | 2       | 21 seconds ago |
| (Tue Nov 14 14:30:49 UTC 2023) |               |         |                |
| Local Fault                    | --            | 2       | 22 seconds ago |
| (Tue Nov 14 14:30:48 UTC 2023) |               |         |                |
| Link State                     | Up            | 1       | 16 seconds ago |
| (Tue Nov 14 14:30:54 UTC 2023) |               |         |                |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.14   | Command introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300P | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show interface profile

show interface [<IFNAME> | <IFRANGE>] profile

## Description

Displays the profile information for each interface.

| Parameter | Description                    |
|-----------|--------------------------------|
| <IFNAME>  | Specifies the interface name.  |
| <IFRANGE> | Specifies the interface range. |

## Examples

Displaying the profile information for each interface:

```
switch# show interface profile

Port Profile Active Profile
Type Membership

...
1/1/17 -- yes --
1/1/17:1 split yes profile-1 profile-2
1/1/17:2 split yes profile-1 profile-2
1/1/17:3 split yes profile-1 profile-2
1/1/17:4 split yes profile-1 profile-2
1/1/18 -- yes --
1/1/18:1 split yes profile-1
1/1/18:2 split yes profile-1
1/1/18:3 split yes profile-1
1/1/18:4 split yes profile-1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                                   |
|---------|------------------------------------------------|
| 10.15   | Command supported on the 9300 Switch Series    |
| 10.14   | Command introduced on the 9300S Switch Series. |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## show interface statistics

```
show interface [<IFNAME>|<IFRANGE>] statistics [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] statistics monitor [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] error-statistics [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] error-statistics monitor [non-zero] [human-readable]
show interface lag [<LAG-ID>] statistics [non-zero] [human-readable]
show interface lag [<LAG-ID>] statistics monitor [non-zero] [human-readable]
show interface lag [<LAG-ID>] error-statistics [non-zero] [human-readable]
show interface lag [<LAG-ID>] error-statistics monitor [non-zero] [human-readable]
show interface vxlan <VXLAN-ID> statistics [non-zero] [human-readable]
```

## Description

Shows statistics for switch interfaces such as packets transmitted and received, bytes transmitted and received, broadcast and multicast packets.

| Parameter      | Description                                                                       |
|----------------|-----------------------------------------------------------------------------------|
| <IFNAME>       | Specifies a interface name.                                                       |
| <IFRANGE>      | Specifies the port identifier range.                                              |
| LAG            | Shows LAG interface information.                                                  |
| <LAG-ID>       | Specifies the LAG number. Range: 1-256                                            |
| VXLAN          | Shows the VXLAN interface information.                                            |
| <VXLAN-ID>     | Specifies the VXLAN interface identifier. Default: 1                              |
| monitor        | Continuously monitor interface statistics.                                        |
| human-readable | Shows statistics rounded to the nearest power of 1000, for example, 1K, 345M, 2G. |

| Parameter | Description                     |
|-----------|---------------------------------|
| non-zero  | Shows only non zero statistics. |

## Examples

Showing statistics of all interfaces:

```
show interface statistics
```

| Interface     | RX Bytes | RX Packets | RX Drops | TX Bytes | TX Packets | TX Drops | RX Broadcast | RX Multicast | TX Broadcast | TX Multicast | RX Pause | TX Pause |
|---------------|----------|------------|----------|----------|------------|----------|--------------|--------------|--------------|--------------|----------|----------|
| 1/1/1         | 2727136  | 1975       | 0        | 17796    | 195        | 0        | 82           | 1788         | 96           | 54           | 0        | 0        |
| 1/1/10        | 0        | 0          | 0        | 0        | 0          | 0        | 0            | 0            | 0            | 0            | 0        | 0        |
| 1/1/11        | 0        | 0          | 0        | 0        | 0          | 0        | 0            | 0            | 0            | 0            | 0        | 0        |
| 1/1/12        | 0        | 0          | 0        | 0        | 0          | 0        | 0            | 0            | 0            | 0            | 0        | 0        |
| ...           |          |            |          |          |            |          |              |              |              |              |          |          |
| 1/1/30 - lag1 | 0        | 0          | 0        | 11271    | 92         | 0        | 0            | 0            | 0            | 51           | 0        | 0        |
| 1/1/31 - lag2 | 2360     | 25         | 50       | 2732119  | 2040       | 0        | 0            | 0            | 178          | 1839         | 0        | 0        |
| 1/1/32 - lag2 | 0        | 0          | 0        | 11373    | 93         | 0        | 0            | 0            | 0            | 51           | 0        | 0        |
| vlan1         | 0        | 0          | 0        | 0        | 0          | 0        | 0            | 0            | 0            | 0            | 0        | 0        |

Showing statistics of all interfaces with only non-zero statistics:

```
show interface statistics non-zero
```

| Interface     | RX Bytes | RX Packets | RX Drops | TX Bytes | TX Packets | TX Drops | RX Broadcast | RX Multicast | TX Broadcast | TX Multicast | RX Pause | TX Pause |
|---------------|----------|------------|----------|----------|------------|----------|--------------|--------------|--------------|--------------|----------|----------|
| 1/1/1         | 2727136  | 1975       | 0        | 17796    | 195        | 0        | 82           | 1788         | 96           | 54           | 0        | 0        |
| 1/1/30 - lag1 | 0        | 0          | 0        | 11271    | 92         | 0        | 0            | 0            | 0            | 51           | 0        | 0        |
| 1/1/31 - lag2 | 2360     | 25         | 50       | 2732119  | 2040       | 0        | 0            | 0            | 178          | 1839         | 0        | 0        |
| 1/1/32 - lag2 | 0        | 0          | 0        | 11373    | 93         | 0        | 0            | 0            | 0            | 51           | 0        | 0        |

Showing statistics of all interfaces in the human-readable format:

```
show interface statistics human-readable
```

| Interface | RX Bytes | RX Pkts | RX Drops | TX Bytes | TX Pkts | TX Drops | RX Bcast | RX Mcast | TX Bcast | TX Mcast | RX Pause | TX Pause |
|-----------|----------|---------|----------|----------|---------|----------|----------|----------|----------|----------|----------|----------|
| 1/1/1     | 744M     | 577K    | 0        | 745M     | 578K    | 0        | 0        | 0        | 73       | 287      | 0        | 0        |
| 1/1/2     | 474M     | 367K    | 0        | 475M     | 369K    | 0        | 0        | 0        | 73       | 288      | 0        | 0        |
| 1/1/3     | 0        | 0       | 0        | 0        | 0       | 0        | 0        | 0        | 0        | 0        | 0        | 0        |

Showing statistics of a single interfaces:

```
show interface 1/1/2 statistics
```

| Interface | RX Bytes | RX Packets | RX Drops | TX Bytes | TX Packets | TX Drops | RX Broadcast | RX Multicast | TX Broadcast | TX Multicast | RX Pause | TX Pause |
|-----------|----------|------------|----------|----------|------------|----------|--------------|--------------|--------------|--------------|----------|----------|
| 1/1/2     | 2725080  | 1931       | 0        | 25877    | 253        | 0        | 21           | 1788         | 65           | 55           | 0        | 0        |

Showing statistics of all members of a LAG interface:

```
show interface lag1 statistics
```

| Interface     | RX Bytes | RX Packets | RX Drops | TX Bytes | TX Packets | TX Drops | RX Broadcast | RX Multicast | TX Broadcast | TX Multicast | RX Pause | TX Pause |
|---------------|----------|------------|----------|----------|------------|----------|--------------|--------------|--------------|--------------|----------|----------|
| 1/1/3 - lag1  | 2424     | 26         | 0        | 2734082  | 2062       | 0        | 0            | 0            | 191          | 1848         | 0        | 0        |
| 1/1/30 - lag1 | 0        | 0          | 0        | 12383    | 100        | 0        | 0            | 0            | 0            | 59           | 0        | 0        |
| lag1          | 2424     | 26         | 0        | 2746465  | 2162       | 0        | 0            | 0            | 191          | 1907         | 0        | 0        |

Showing error statistics of all interfaces:



```
show interface error-statistics
```

| Interface     | RX Errors | TX Errors | Giants | Runts | CRC/FCS | Collisions |
|---------------|-----------|-----------|--------|-------|---------|------------|
| 1/1/1         | 190       | 20        | 100647 | 0     | 0       | 0          |
| 1/1/10        | 0         | 0         | 100    | 290   | 7165    | 949        |
| 1/1/11        | 0         | 0         | 0      | 0     | 0       | 0          |
| 1/1/12        | 0         | 0         | 0      | 0     | 0       | 0          |
| ...           |           |           |        |       |         |            |
| 1/1/30 - lag1 | 1500      | 500       | 45800  | 0     | 0       | 0          |
| 1/1/31 - lag2 | 0         | 0         | 11     | 27    | 0       | 0          |
| 1/1/32 - lag2 | 0         | 0         | 0      | 0     | 6       | 18         |

Showing monitor statistics:



The rows and columns of show interface monitor statistics depends on the length of width of the client terminal. The CLI can be navigated using the arrow keys as well as the PageUp, PageDown, Home, and End keys.

```
show interface statistics monitor
```

| Interface | RX Bytes      | RX Packets >> |
|-----------|---------------|---------------|
| 1/1/1     | 3440525421984 | 53758209526   |
| 1/1/2     | 3440526607008 | 53758228042   |
| 1/1/3     | 3440527785312 | 53758246453   |
| 1/1/30    | 3440559671264 | 53758744653   |
| 1/1/31    | 3440560851680 | 53758763098   |
| 1/1/32    | 3440562028704 | 53758781489   |

help: ?, quit: q

Help for Interface Monitor

f Toggle full statistics  
h Toggle human-readable mode  
n Toggle non-zero mode  
r Toggle rate display

c Clear interface statistics  
Does not apply to rates

Arrows, PgUp, PgDn, Home, End  
Navigate interface statistics

Delay:2

help: ?, qui

Showing monitor error statistics in human-readable format:

```
show interface 1/1/1-1/1/3,1/1/30-1/1/32 error-statistics monitor human-readable
```

| Interface | RX Errors | TX Errors | RX Giants | RX Runts | CRC/FCS | Collisions |
|-----------|-----------|-----------|-----------|----------|---------|------------|
| 1/1/1     | 0         | 0         | 0         | 0        | 0       | 0          |
| 1/1/2     | 0         | 0         | 0         | 0        | 0       | 0          |
| 1/1/3     | 0         | 0         | 0         | 0        | 0       | 0          |
| 1/1/30    | 0         | 0         | 0         | 0        | 0       | 0          |
| 1/1/31    | 0         | 0         | 0         | 0        | 0       | 0          |
| 1/1/32    | 0         | 0         | 0         | 0        | 0       | 0          |

```
Human-readable help: ?, quit: q
```

```
Help for Interface Monitor
```

```
h Toggle human-readable mode
n Toggle non-zero mode

c Clear interface statistics
 Does not apply to rates

Arrows, PgUp, PgDn, Home, End
 Navigate interface statistics

Delay:2 help: ?, quit: q
```



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

## Command History

| Release          | Modification                                 |
|------------------|----------------------------------------------|
| 10.11            | Added <code>monitor</code> parameter.        |
| 10.10            | Added <code>human-readable</code> parameter. |
| 10.07 or earlier | --                                           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show interface transceiver

```
show interface [<INTERFACE-ID>] transceiver [detail | threshold-violations] [vsx-peer]
```

### Description

Displays information about transceivers present in the switch. The information shown varies for different transceiver types and manufacturers. Only basic information is shown for unsupported HPE

and third-party transceivers installed in the switch and they are also identified with an asterisk in the output.

| Parameter            | Description                                                                                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-ID>       | Specifies the name or range of an interface on the switch. Use the format <b>member/slot/port</b> (for example, <b>1/3/1</b> ).                                                                                                  |
| detail               | Show detailed information for the interfaces.                                                                                                                                                                                    |
| threshold-violations | Show threshold violations for transceivers.                                                                                                                                                                                      |
| vsx-peer             | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

Showing summary transceiver information with identification of unsupported transceivers:

```
switch(config)# show interface transceiver

Port Type Product Serial Part
Number Number Number

1/1/1 SFP+SR J9150A MYxxxxxxx 1990-3657
1/1/2 SFP+ER* -- -- --
1/2/1 QSFP+SR4 JH233A MYxxxxxxx 2005-1234
1/2/2 QSFP+ER4* -- -- --
1/3/1 SFP28DAC3 844477-B21 MYxxxxxxx 77fc-7ce7
* unsupported transceiver
```

Showing detailed transceiver information:

```
switch(conf#) show interface transceiver detailing
Transceiver in 1/1/1
 Interface Name : 1/1/1
 Type : SFP+SR
 Connector Type : LC
 Wavelength : 850nm
 Transfer Distance : 0m (SMF), 30m (OM1), 80m (OM2), 300m (OM3)
 Diagnostic Support : DOM
 Product Number : J9150A
 Serial Number : MYxxxxxxx
 Part Number : 1990-3657

Status
 Temperature : 47.65C
 Voltage : 3.31V
 Tx Bias : 8.40mA
 Rx Power : 0.08mW, -10.96dBm
 Tx Power : 0.56mW, -2.49dBm

Recent Alarms :
 Rx power low alarm
 Rx power low warning
```

```

Recent Errors :
Rx loss of signal

Transceiver in 1/1/2
Interface Name : 1/1/2
Type : unknown
Connector Type : ??
Wavelength : ??
Transfer Distance : ??
Diagnostic Support : ??
Product Number : ??
Serial Number : ??
Part Number : ??

Transceiver in 1/2/1
Interface Name : 1/2/1
Type : QSFP+SR4
Connector Type : MPO
Wavelength : 850nm
Transfer Distance : 0m (SMF), 0m (OM1), 0m (OM2), 100m (OM3)
Diagnostic Support : DOM
Product Number : JH233A
Serial Number : MYxxxxxxx
Part Number : 2005-1234

Status
Temperature : 44.46C
Voltage : 3.30V

Channel# Tx Bias Rx Power Tx Power
 (mA) (mW/dBm) (mW/dBm)

1 6.12 0.00, -inf 0.63, -1.95
2 6.04 0.00, -inf 0.63, -2.00
3 6.51 0.00, -inf 0.60, -2.16
4 6.19 0.00, -inf 0.63, -1.94

Recent Alarms :
Channel 1 :
 Rx power low alarm
 Rx power low warning
Channel 2 :
 Rx power low alarm
 Rx power low warning
Channel 3 :
 Rx power low alarm
 Rx power low warning
Channel 4 :
 Rx power low alarm
 Rx power low warning

Recent Errors :
Channel 1 :
 Rx Loss of Signal
Channel 2 :
 Rx Loss of Signal
Channel 3 :
 Rx Loss of Signal
Channel 4 :
 Rx Loss of Signal

```

```

Transceiver in 1/2/2
 Interface Name : 1/2/2
 Type : unknown
 Connector Type : ??
 Wavelength : ??
 Transfer Distance : ??
 Diagnostic Support : ??
 Product Number : ??
 Serial Number : ??
 Part Number : ??

Transceiver in 1/3/1
 Interface Name : 1/3/1
 Type : SFP28DAC3
 Connector Type : Copper Pigtail
 Transfer Distance : 0.00km (SMF), 0m (OM1), 0m (OM2), 0m (OM3)
 Diagnostic Support : None
 Product Number : 844477-B21
 Serial Number : MYxxxxxxx
 Part Number : 77fc-7ce7

```

Showing detailed transceiver information with identification of unsupported transceivers:

```

Transceiver in 1/1/2
 Interface Name : 1/1/2
 Type : SFP+ER (unsupported)
 Connector Type : LC
 Wavelength : 3590nm
 Transfer Distance : 80m (SMF), 0m (OM1), 0m (OM2), 0m (OM3)
 Diagnostic Support : DOM
 Vendor Name : INNOLIGHT
 Vendor Part Number : TR-PX15Z-NHP
 Vendor Part Revision : 1A
 Vendor Serial number : MYxxxxxxx

Status
 Temperature : 28.88C
 Voltage : 3.30V
 Tx Bias : 65.53mA
 Rx Power : 0.00mW, -inf
 Tx Power : 1.47mW, 1.67dBm

Recent Alarms:
 Rx Power low alarm
 Rx Power low warning
Recent Errors:

```

Showing transceiver threshold-violations:

```

switch(config)# show interface transceiver threshold-violations

Port Type Channel Type(s) of Recent
 Threshold Violation(s)

1/1/1 SFP+SR Tx bias high warning
 50.52 mA > 40.00 mA
1/1/2 SFP+ER* ??
1/2/1 QSFP+SR4 1 Tx power low alarm

```

```
2 -17.00 dBm < -0.50 dBm
Tx bias low warning
3.12 mA < 4.00 mA
??
n/a
1/2/2 QSFP+ER4*
1/3/1 SFP28DAC3
* unsupported transceiver
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show interface supported-transceivers

```
show interface {<IFNAME>|<IFRANGE>} supported-transceivers
```

## Description

Displays transceivers supported by a specific, or all, interface(s) in the switch. Information varies and is dependent on transceiver types, part number, and short description or interfaces.

| Parameter      | Description                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| <i>IFNAME</i>  | Specifies the name of an interface on the switch.<br>Use the following format: member/slot/port.<br>Example: 1/3/1             |
| <i>IFRANGE</i> | Specifies the name of an interface range on the switch.<br>Use the following format: member/slot/port.<br>Example: 1/1/1-1/1/2 |

## Example

Showing a full switch interface or chassis switch with multiple line modules:

```
switch# show interface supported-transceivers
```

| Type       | Product Number | Supported Interfaces                                                                                        |
|------------|----------------|-------------------------------------------------------------------------------------------------------------|
| 1G-BT      | JL747          | 1/1/33-1/1/34                                                                                               |
| 1G-BT      | J8177          | 1/1/33-1/1/34                                                                                               |
| 1G-LH      | J4860          | 1/1/33-1/1/34                                                                                               |
| 1G-LX      | J4859          | 1/1/33-1/1/34                                                                                               |
| 8x25G-DAC2 | S4B39          | 1/1/2,1/1/4,1/1/6,1/1/8,1/1/10,1/1/12,1/1/14,1/1/16,1/1/18,1/1/20,1/1/22,1/1/24,1/1/26,1/1/28,1/1/30,1/1/32 |
| QSA28      | 845970         | 1/1/1-1/1/32                                                                                                |

Note: For full product numbers (SKUs) with revision letters, refer to the transceiver guide.

```
switch# show interface supported-transceivers
```

| Type          | Product Number | Supported Interfaces                                                                                                           |
|---------------|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| 100M-FX       | J9054          | 1/10/1-1/10/24,1/12/1-1/12/48                                                                                                  |
| 1G-BT         | JL747          | 1/5/49-1/5/52,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48                                          |
| 10G-BT        | JL563          | 1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48                             |
| 10G-BiDi-D    | R9X54          | 1/4/1-1/4/12,1/6/1-1/6/36,1/11/1-1/11/12,1/12/1-1/12/48                                                                        |
| 10G-SR        | J9150          | 1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,1/11/1-1/11/12,1/12/1-1/12/48 |
| 10G-SR        | JL782          | 1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12                                                                                      |
| 25G-AOC15     | R0Z21          | 1/6/1-1/6/32                                                                                                                   |
| 25G-AOC7      | R0M45          | 1/6/1-1/6/32                                                                                                                   |
| 25G-BiDi-10-U | S1C98          | 1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/25-1/10/28,1/12/1-1/12/48               |
| 8x50G-DAC2    | S4B42          | 1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/25-1/10/28,1/12/1-1/12/48                            |
| QSA28         | 845970         | 1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12                                                                                      |

Note: For full product numbers (SKUs) with revision letters, refer to the transceiver guide.

Showing a single interface:

```
switch# show interface 1/1/1 supported-transceivers
```

| Type            | Product Number | Description       |
|-----------------|----------------|-------------------|
| Interface 1/1/1 |                |                   |
| 10G-BiDi-D @    | R9X54          | 10G BX-D 40km     |
| 10G-BiDi-U @    | R9X55          | 10G BX-U 40km     |
| 100G-LR4        | JL310          | 100G QSFP28 LR4   |
| 100G-SR1.2      | S4B44          | 100G SR1.2 Q28 LC |
| 100G-SR2        | S1C93          | 100G MPO SR2      |
| 100G-SR4        | JL309          | 100G QSFP28 SR4   |
| QSA28           | 845970         | --                |

@ This transceiver is only supported when inserted in a QSA

For full product numbers (SKUs) with revision letters, refer to the Transceiver guide.

Showing a range of interfaces:

```
switch# show interface 1/1/1-1/1/2 supported-transceivers
```

| Type            | Product Number | Description     |
|-----------------|----------------|-----------------|
| Interface 1/1/1 |                |                 |
| 10G-BiDi-D @    | R9X54          | 10G BX-D 40km   |
| 10G-BiDi-U @    | R9X55          | 10G BX-U 40km   |
| 10G-ER @        | S2P32          | 10G SFP+ ER     |
| 100G-SR2        | S1C93          | 100G MPO SR2    |
| 100G-SR4        | JL309          | 100G QSFP28 SR4 |
| QSA28           | 845970         | --              |
| Interface 1/1/2 |                |                 |

|                 |        |                    |
|-----------------|--------|--------------------|
| 10G-BiDi-D @    | R9X54  | 10G BX-D 40km      |
| 10G-BiDi-U @    | R9X55  | 10G BX-U 40km      |
| 10G-ER @        | S2P32  | 10G SFP+ ER        |
| 25G-BiDi-10-D @ | S1C96  | 25G LC BiDi 10km-D |
| 25G-SR @        | S2P33  | 25G SFP28 SR       |
| 40G-eSR4        | JH233  | QSFP+ eSR4         |
| 100G-BiDi       | 845972 | --                 |
| 100G-SR4        | JL309  | 100G QSFP28 SR4    |
| QSA28           | 845970 | --                 |

@ This transceiver is only supported when inserted in a QSA

For full product numbers (SKUs) with revision letters, refer to the Transceiver guide.

Showing a chassis switch with multiple line modules:

```
switch# show interface supported-transceivers
```

| Type       | Product Number | Supported Interfaces                                                                                                                   |
|------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 100M-FX    | J9054          | 1/10/1-1/10/24,1/12/1-1/12/48                                                                                                          |
| 1G-BT      | JL747          | 1/5/49-1/5/52,1/7/25-1/7/28,1/8/25-1/8/28,<br>1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48                                              |
| 10G-BT     | JL563          | 1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,<br>1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,<br>1/12/1-1/12/48                             |
| 10G-BiDi-D | R9X54          | 1/4/1-1/4/12,1/6/1-1/6/36,1/11/1-1/11/12,<br>1/12/1-1/12/48                                                                            |
| 10G-SR     | J9150          | 1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,<br>1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,<br>1/10/1-1/10/28,1/11/1-1/11/12,1/12/1-1/12/48 |
| 10G-SR     | JL782          | 1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12                                                                                              |
| 25G-AOC15  | R0Z21          | 1/6/1-1/6/32                                                                                                                           |
| 25G-AOC7   | R0M45          | 1/6/1-1/6/32                                                                                                                           |



```

25G-BiDi-10-U S1C98 1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,
8x50G-DAC2 S4B42 1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,
 1/8/25-1/8/28,1/9/49-1/9/52,1/10/25-1/10/28,
 1/12/1-1/12/48
QSA28 845970 1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12

For full product numbers (SKUs) with revision letters, refer to the Transceiver
guide.

```

Showing a VSF stack:

```

switch# show interface supported-transceivers

Type Product Supported
 Number Interfaces

100M-FX J9054 1/1/1-1/1/24,2/1/1-2/1/48
1G-BT JL747 1/1/49-1/1/52,3/1/25-3/1/28,4/1/25-4/1/28
10G-BT JL563 1/1/49-1/1/52,2/1/1-2/1/32,3/1/25-3/1/28,
 4/1/25-4/1/28
10G-AOC15 721076 1/1/13,1/1/15-1/1/27,1/1/41-1/1/42
10G-AOC5 Q9S66 1/1/13,1/1/15-1/1/27,1/1/41-1/1/42
25G-AOC15 R0Z21 3/1/1-3/1/32
QSA28 845970 4/1/1-4/1/12,2/1/33-2/1/36,1/1/1-1/1/12

For full product numbers (SKUs) with revision letters, refer to the Transceiver
guide.

```

Showing an empty chassis:

```

switch# show interface supported-transceivers
No available interfaces.

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification       |
|------------|--------------------|
| 10.16.1000 | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show interface utilization

show interface [*<IFNNAME>* | *<IFRANGE>*] utilization [non-zero]

## Description

Displays physical port throughput and utilization.

| Parameter              | Description                          |
|------------------------|--------------------------------------|
| <i>&lt;IFNAME&gt;</i>  | Specifies an interface name.         |
| <i>&lt;IFRANGE&gt;</i> | Specifies the port identifier range. |
| utilization            | Displays utilization statistics.     |
| non-zero               | Displays non-zero statistics         |

## Examples

The following example shows port utilization of all interfaces:

```
switch# show interface utilization
-----|-----|-----|-----
Interval | RX | TX | Total (RX+TX) |
Interface seconds | Mbps Kpkt/s Util % | Mbps Kpkt/s Util % | Mbps
Kpkt/s Util % | Description
-----|-----|-----|-----
1/1/1 300 9578.02 788.70 95.78 25.70 45.89 0.26 9603.72
834.59 96.04 Aruba-AP
1/1/2 300 25.71 45.90 0.26 9581.09 788.96 95.81 9606.80
834.86 96.07 Aruba2530-AP-conce...
1/1/3 - lag123 300 0.00 0.00 0.00 0.00 0.00 0.00 0.00
0.00 0.00 ISL: SWRTS-0064-1
1/1/4 300 9261.79 804.52 92.62 9496.70 823.97 94.97 18758.50
1628.48 187.58 Backup data center...
1/1/5 300 9496.70 823.97 94.97 9261.79 804.52 92.62 18758.50
1628.48 187.58 --
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip interface

show ip interface <INTERFACE-ID>[{lag|loopback|vlan|tunnel <ID>}]

### Description

Shows status and configuration information for an IPv4 interface.

| Parameter      | Description                                                           |
|----------------|-----------------------------------------------------------------------|
| <INTERFACE-ID> | Specifies the name of an interface. Format: <b>member/slot/port</b> . |
| lag <ID>       | Show LAG interface information, where <ID> is 1-256.                  |
| loopback <ID>  | Show loopback interface information, where <ID> is 0-255.             |
| tunnel <ID>    | Show tunnel interface information, where <ID> is 1-255.               |
| vlan <ID>      | Show VLAN interface information, where <ID> is 1-4094.                |

### Example

```
switch# show ip interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IP MTU 1500
IP TCP MSS 1460
IPv4 address 192.168.1.1/24
```

```
switch# show ip interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IP MTU 1500
IP TCP MSS 1460
IP Directed Broadcast is Disabled
IPv4 address 2.2.2.2/32 [unnumbered to loopback1]
L3 Counters: Rx Disabled, Tx Disabled
```

```
switch# show ip interface loopback 1
Interface loopback1 is up
Admin state is up
Hardware: Loopback
IP Directed Broadcast is Disabled
IPv4 address 192.168.1.1/24
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                                                        |
|------------------|-----------------------------------------------------------------------------------------------------|
| 10.14.1000       | Command output can display information for an IP unnumbered interface and IP TCP MSS configuration. |
| 10.07 or earlier | --                                                                                                  |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip source-interface

```
show ip source-interface {sflow | tftp | radius | tacacs | all} [vrf <VRF-NAME>]
[vsx-peer]
```

### Description

Shows single source IP address configuration settings.

| Parameter                            | Description                                                                                                                                                                                                                      |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sflow   tftp   radius   tacacs   all | Shows single source IP address configuration settings for a specific protocol. The <b>all</b> option shows the global setting that applies to all protocols that do not have an address set.                                     |
| vrf <VRF-NAME>                       | Specifies the name of a VRF.                                                                                                                                                                                                     |
| vsx-peer                             | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

```
Showing single source IP address configuration settings for sFlow:
switch# show ip source-interface sflow
Source-interface Configuration Information

Protocol Source Interface

sflow 10.10.10.1
```

Showing single source IP address configuration settings for all protocols:

```
switch# show ip source-interface all
Source-interface Configuration Information

Protocol Source Interface

all 1/1/1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show ipv6 interface

show ipv6 interface <INTERFACE-ID> [vsx-peer]

## Description

Shows status and configuration information for an IPv6 interface.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-ID> | Specifies an interface ID. Format: <b>member/slot/port</b> .                                                                                                                                                                     |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

```
switch# show ipv6 interface 1/1/1
Interface 1/1/1 is up
Admin state is up
IPv6 address:
 2001:0db8:85a3:0000:0000:8a2e:0370:7334/24 [VALID]
IPv6 link-local address: fe80::1e98:ecff:fee3:e800/64 (default) [VALID]
IPv6 virtual address configured: none
IPv6 multicast routing: disable
IPv6 Forwarding feature: enabled
IPv6 multicast groups locally joined:
```

```
ff02::ff70:7334 ff02::ffe3:e800 ff02::1 ff02::1:ff00:0
ff02::2
IPv6 multicast (S,G) entries joined: none
IPv6 MTU: 1524 (using link MTU)
IPv6 TCP MSS 1440
IPv6 unicast reverse path forwarding: none
IPv6 load sharing: none
RX
 0 packets, 0 bytes
TX
 0 packets, 0 bytes
```

```
switch# show ipv6 interface 1/1/14.1
Interface 1/1/14.1 is up
Admin state is up
IPv6 address:
 30::1/64 [VALID]
IPv6 link-local address: fe80::b86a:97c0:122:2f42/64 [VALID]
IPv6 virtual address configured: none
IPv6 multicast routing: disable
IPv6 Forwarding feature: enabled
IPv6 multicast groups locally joined:
 ff02::1 ff02::1:ff22:2f42 ff02::1:ff00:1 ff02::1:ff00:0
 ff02::2
IPv6 multicast (S,G) entries joined: none
IPv6 MTU 1500
IPv6 TCP MSS 1440
IPv6 unicast reverse path forwarding: none
IPv6 load sharing: none
Encapsulation dot1q ID: 20
```

```
switch# show ipv6 interface lag2.1
Interface lag2.1 is up
Admin state is up
IPv6 address:
 40::1/64 [VALID]
IPv6 link-local address: fe80::b86a:97c0:122:2f42/64 [VALID]
IPv6 virtual address configured: none
IPv6 multicast routing: disable
IPv6 Forwarding feature: enabled
IPv6 multicast groups locally joined:
 ff02::1 ff02::1:ff22:2f42 ff02::1:ff00:1 ff02::1:ff00:0
 ff02::2
IPv6 multicast (S,G) entries joined: none
IPv6 MTU 1500
IPv6 TCP MSS 1440
IPv6 unicast reverse path forwarding: none
IPv6 load sharing: none
Encapsulation dot1q ID: 30
```



---

For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

---

## Command History

| Release          | Modification                                                                                          |
|------------------|-------------------------------------------------------------------------------------------------------|
| 10.14.1000       | Command output can display information for an IP unnumbered interface and IPv6 TCP MSS configuration. |
| 10.07 or earlier | --                                                                                                    |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ipv6 source-interface

```
show ipv6 source-interface <PROTOCOL> [{all-vrfs | vrf <VRF-NAME>}]
[vsx-peer]
```

### Description

Shows single source IPv6 address configuration settings.

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <PROTOCOL>                | <p>Specifies the protocol to configure.</p> <ul style="list-style-type: none"> <li>▪ <b>all</b>: Selects the source for all protocols covered by this command.</li> <li>▪ <b>central</b>: Selects HPE Aruba Networking Central.</li> <li>▪ <b>dhcp_relay</b>: Selects DHCP relay. When you configure a dhcp_relay source interface, you must also enable DHCP relay Option 82 using the <b>dhcp-relay option 82source-interface</b> command.</li> <li>▪ <b>dns</b>: Selects DNS.</li> <li>▪ <b>http</b>: Selects HTTP.</li> <li>▪ <b>ipfix</b>: Selects ipfix. Configures source interface for IPFIX.</li> <li>▪ <b>ntp</b>: Selects NTP.</li> <li>▪ <b>radius</b>: Selects RADIUS.</li> <li>▪ <b>sflow</b>: Selects sFlow.</li> <li>▪ <b>sftp-scp</b>: Selects SFTP and SCP.</li> <li>▪ <b>ssh-client</b>: Selects SSH Client.</li> <li>▪ <b>syslog</b>: Selects the source for syslog packets.</li> <li>▪ <b>tacacs</b>: Selects the source for TACACS packets.</li> <li>▪ <b>tftp</b>: Selects TFTP.</li> </ul> |
| all-vrfs   vrf <VRF-NAME> | Specifies the name of a VRF.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| vsx-peer                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

### Examples

Showing single source IPv6 address configuration settings for sFlow:

```
switch# show ipv6 source-interface sflow

Source-interface Configuration Information

Protocol Source Interface

sflow 2001:DB8::1
```

Showing single source IPv6 address configuration settings for all protocols:

```
switch# show ipv6 source-interface all

Source-interface Configuration Information

Protocol Source Interface

all 1/1/1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show system interface-group

```
show system interface-group
 detail
 line-module <slot-id>

 member <member-id>
```

## Description

Displays the configuration and status of interface groups.

| Parameter     | Description                               |
|---------------|-------------------------------------------|
| <i>detail</i> | Show detailed interface group information |



| Parameter                                | Description                                                            |
|------------------------------------------|------------------------------------------------------------------------|
| <code>line-module &lt;slot-id&gt;</code> | Show information for a line module slot ID (for example, <b>1/1</b> ). |
| <code>member &lt;member-id&gt;</code>    | Show information for a single VSF member                               |

## Examples



The output in the following commands vary, depending on switch model.

Show basic interface group status

```
switch# show system interface-group

Group Speed Member Ports Mismatched Ports

1 10g 1/1/1-1/1/12
2 25g 1/1/13-1/1/24 1/1/13
3 25g 1/1/25-1/1/36
4 25g 1/1/37-1/1/48
```

Show detailed interface group status, including allowed speeds of each.

```
switch# show system interface-group detail

Allowed Mismatched
Module Group Ports Option Speeds Ports

1/6 1 1-8 25g @+* 10g,25g
50g 50g
1/6 2 9-16 25g * 10g,25g
50g @+ 50g 9-16
1/6 3 17-24 25g @+* 10g,25g
50g 50g
1/6 4 25-32 25g * 10g,25g
50g @+ 50g
@ Currently applied setting
+ Configured setting
* Default setting
```
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300S 10040	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show system interface-profile

show system interface-profile

Description

Displays the configuration and status of interface profiles.

Examples

Displaying the configuration and status of the system interface profile.

```
switch# show system interface-profile
-----
Module  Profile      Default      Configured    Active
Type    Profile      Profile      Profile      Profile
-----
1/1     split        profile-1    profile-1     profile-1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.15	Command supported on the 9300 Switch Series
10.14	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

shutdown

shutdown
no shutdown

Description

Disables an interface. Interfaces are disabled by default when created.

The **no** form of this command enables an interface.

Examples

Disabling an interface:

```
switch(config-if) # shutdown
```

Enabling an interface:

```
switch(config-if) # no shutdown
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

system interface-group

```
system interface-group <GROUP> speed <SPEED>  
no system interface-group <GROUP> speed <SPEED>
```

Description

Configures the speed for an interface group. After changing group speed, only transceivers compatible with the new speed will be enabled.



- All speed-mismatched interfaces in the group will be disabled.
- This command can interrupt active network links, user confirmation is required to proceed.

The **no** form of this command resets the specified interface group to its default.

Parameter	Description
<GROUP>	Specifies the interface group to configure.

Parameter	Description
<SPEED>	Configures transceiver speed (10g or 25g) for a group. Default is 25g (see the Transceiver Guide for further detail). On HPE Aruba Networking 9300/9300S Switch Series: 10g allows 1Gbps or 10Gbps transceivers only. 25g allows 25Gbps transceivers only.

Usage

Some switch models have a restriction that all ports in a group of ports must have compatible speeds. The table below shows the port groups for all models with this restriction:

Model	Group	Ports	Default Speeds	Alternate Speeds	
9300S S0F96A	1	4-Jan	25/100Gbps only	10/40Gbps only	
	2	8-May	25/100Gbps only	10/40Gbps only	
	3	12-Sep	25/50/100/200Gbps only	10/40Gbps only	
	4	13-16	25/50/100/200Gbps only	10/40Gbps only	
	5	25-28	25/50/100/200Gbps only	10/40Gbps only	
	6	29-32	25/50/100/200Gbps only	10/40Gbps only	
	7	33-36	25/100Gbps only	10/40Gbps only	
	8	37-40	25/100Gbps only	10/40Gbps only	
100040 S4R58A S4R59A	1	4-Jan	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	2	8-May	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	3	12-Sep	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	4	13-16	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	5	17-20	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	6	21-24	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	7	25-28	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only
	8	29-32	25/100Gbps only	25/50/100/200Gbps only*	10/40Gbps only

* The odd-numbered ports of the group are unavailable when this speed is configured.

Examples

Configuring interface group 1 to allow 10Gbps and slower transceivers:

```
switch(config)# system interface-group 1 speed 10g
Changing the group speed will disable all member interfaces that do not match the
new speed.

Continue (y/n)? y
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.10.1000	Command introduced on 9300 and 10000 Switch series.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

system interface-profile

```
system interface-profile
  encryption <NAME>
  no ..
  split <NAME>`
```

Description

Configures an interface profile with an encryption or interface group profile, or defines a splittable interface.

The **no** form of this command removes the specified interface profile.

Parameter	Description
encryption <name> <NAME>	Encryption profiles are used to select different sets of ports that support MACsec encryption/decryption. Because hardware resources are limited for the aggregate bandwidth available for MACsec, the switch has different MACsec profiles that are designed to maximize the number of ports that can be used based on network requirements. When setting an encryption profile, it will only change the

Parameter	Description
	configured profile and not the active profile. A reboot is required to make the new profile active and change the MACsec capable ports.
<code>split <NAME></code>	Configures a splittable interface profile on 9300, 9300S and 10040 Switch series, where <name> specifies one of the following two profile names: ▪ profile-1 ▪ profile-2

Usage

Some switch models have hardware resource allocation options for different applications. For example, a switch that cannot support splitting all ports for use with breakout cables may have a profile to maximize 100G links and another profile to maximize 25G links.

Switch Model	Profile Name	Splittable Ports	Split Modes Available
9300	profile-1 (default)	1-32	2 x 100/200G, 4 x 10/25/50/100G
	profile-2	2-32 even	2 x 100/200G, 4 x 10/25/50/100G, 8 x 10/25/50G* NOTE: Only QSFP-DD ports can split eight ways
9300S	profile-1 (default)	9-12 17-24 29-32	2 x 100G 2 x 100/200G, 4 x 10/25/50/100G 2 x 100G
	profile-2	13, 15, 16 17, 19, 21, 23 25, 26, 27	4 x 10/25G 2 x 100/200G, 4 x 10/25/50/100G 4 x 10/25G

Splittable ports from any profile can always be configured as split interfaces, but the children can only establish a link when the switch is booted with a profile where that port is splittable. For example, port 1/1/16 can be split at any time, but only establishes a link on the child interfaces when the switch is booted with **profile-2** configured. Child ports that are not members of the booted profile remain down with a reason of **Split profile mismatch**.

After changing the configured profile, the switch must be rebooted before that profile is applied. Configuring a new profile does not change the configured split setting for any interfaces. It also does not affect any split interfaces that are not members of the new profile until the switch is rebooted.

Examples

Configuring the switch to use 4x100g breakout cables in ports 17-20:

```
switch(config)# system interface-profile split profile-1
switch(config)# interface 1/1/17-1/1/20
switch(config-if-<1/1/17-1/1/20>)# split 4 100g
```

Configuring the switch to use 4x25g breakout cables in port 16:

```
switch(config)# system interface-profile split profile-2
This command requires a reboot to apply. After reboot, any ports not compatible
with the new profile will be disabled.
Continue (y/n)? y

switch(config)# interface 1/1/16
switch(config-if-<1/1/16>)# split 4 25g
```

Configuring the switch to use 2x100g breakout cables in port 9-12:

```
switch(config)# system interface-profile split profile-1
This command requires a reboot to apply. After reboot, any ports not compatible
with the new profile will be disabled.
Continue (y/n)? y

switch(config)# interface 1/1/9-1/1/12
switch(config-if-<1/1/9-1/1/12>)# split 2 100g
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

copy support-file feature

copy support-file feature 13

Description

Captures support logs to debug any IP Directed Broadcast issues.

Examples

Capturing the support logs into a local file:

```
switch# copy support-file feature 13 sftp
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

ip directed-broadcast

ip directed-broadcast
no ip directed-broadcast

Description

Turns on IP Directed Broadcast for the specified interface. The **no** form of this command turns it off. This command is disabled by default.

Examples

Enabling and disabling IP Directed Broadcast on an physical interface:


```
switch(config)# interface 1/1/1
switch(config-if)# ip directed-broadcast
switch(config-if)# no ip directed-broadcast
```

Enabling and disabling IP Directed Broadcast on a VLAN interface:

```
switch(config)# interface vlan 100
switch(config-if-vlan)# ip directed-broadcast
switch(config-if-vlan)# no ip directed-broadcast
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show arp

show arp

Description

Shows IP directed broadcast verification.



IP Directed Broadcast is not supported on subinterfaces on 8100, 6300, 6400, 8325, 8360 and 10000 Switch series.

Examples

Showing IP directed broadcast verification:

```
switch# show arp
IPv4 Address      MAC                Port      Physical Port      State
-----
1.1.1.255         FF:FF:FF:FF:FF:FF 1/1/1     1/1/1              permanent
3.1.1.255         FF:FF:FF:FF:FF:FF vlan10     vlan10              permanent

Total Number Of ARP Entries Listed: 2.
-----
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip interface

show ip interface <INTERFACE-NAME>

Description

Displays the status of IP Directed Broadcast on the specified interface along with other interface related attributes.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to use as a source for displaying the status of the IP Directed Broadcast.

Examples

Displaying the IP Directed Broadcast status on the specified interface:

```
switch# show ip interface vlan30
```

```
Interface vlan30 is up
Admin state is up
Hardware: Ethernet, MAC Address: 94:f1:28:21:63:00
IP MTU 1500
IP Directed Broadcast is Enabled
IPv4 address 192.168.3.1/24
L3 Counters: Rx Disabled, Tx Disabled
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip directed-broadcast

show ip directed-broadcast

Description

Displays the summary of the interfaces on which IP Directed Broadcast is enabled.

Examples

On the HPE Aruba Networking 6400 Switch Series, interface identification differs.

Displaying the summary of the interfaces on which IP Directed Broadcast is enabled:

```
switch# show ip directed-broadcast

IPv4 Directed Broadcast Configuration

Interface      Status
-----
1/1/1          Enabled
vlan10         Enabled
vlan30         Enabled
```

Displaying IP Directed Broadcast Host entries installed in Neighbor cache:

```
switch# show arp state permanent

IPv4 Address      MAC              Port      Physical Port  State
-----
52.1.1.255        FF:FF:FF:FF:FF:FF 1/1/1     1/1/1          permanent
40.0.0.255        FF:FF:FF:FF:FF:FF vlan20     vlan20          permanent
Total Number Of ARP Entries Listed- 2.
-----
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip neighbor-flood

ip neighbor-flood

Description

Enables VLAN flooding for the specified VLAN interface when a neighbor link goes down. The **no** form of this command disables VLAN flooding for the specified VLAN interface.

Examples

Enabling IP Neighbor Flood on a VLAN interface:

```
switch(config)# interface vlan 3
switch(config-if-vlan)# ip neighbor-flood
```

Disabling IP Neighbor Flood on a VLAN interface.

```
switch(config)# interface vlan 3
switch(config-if-vlan)# no ip neighbor-flood
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

show ip interface

show ip interface <IFNAME>

Description

Displays the status of IP Neighbor Flood on the specified interface along with other interface-related attributes.

Parameter	Description
<code><IFNAME></code>	Specifies the interface name (for example, <code>vlan30</code>). Optional.

Examples

```
switch# show ip interface vlan30

Interface vlan30 is up
Admin state is up
Hardware: Ethernet, MAC Address: 94:f1:28:21:63:00
IP MTU 1500
IP Neighbor Flood is Enabled
IPv4 address 192.168.3.1/24
L3 Counters: Rx Disabled, Tx Disabled
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip neighbor-flood

```
show ip neighbor-flood
```

Description

Displays the interfaces on which IP Neighbor Flood is enabled.

Examples

```
switch# show ip neighbor-flood

IP Neighbor Flood Configuration

Interface      Status
-----
```

vlan10	Enabled
vlan30	Enabled



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config

show running-config

Description

Displays the current running configuration.

Examples

```
switch# show running-config
interface vlan10
    ip neighbor-flood
interface vlan30
    ip neighbor-flood
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

http

```
http {get | raw} <URL> [history-interval <HISTORY-INTERVAL>] [cache disable] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}] [probe-interval <PROBE-INTERVAL>] [proxy <PROXY-URL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|<IFNAME>}] [source-port <SOURCE-PORT-NUM>] [version <VERSION-NUMBER>] [http-raw-request <RAW-PAYLOAD>]
```

```
no http {get | raw} <URL> [history-interval <HISTORY-INTERVAL>] [cache disable] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}] [probe-interval <PROBE-INTERVAL>] [proxy <PROXY-URL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|<IFNAME>}] [source-port <SOURCE-PORT-NUM>] [version <VERSION-NUMBER>] [http-raw-request <RAW-PAYLOAD>]
```

Description

Configures HTTP as the IP-SLA test mechanism. Requires destination URL and type of HTTP request (raw/get).

The **no** version of this command disables HTTP as the IP-SLA test mechanism.

Parameter	Description
{get raw}	Selects HTTP request type as get or raw where the system will generate or provide HTTP payload.
<URL>	Specifies HTTP URL address of syntax http://<HOST NAME/IP-ADDRESS>:<PORT>/<PATH>.
history-interval <HISTORY-INTERVAL>	Configures the history interval for the IP-SLA. Set the history interval to minimum of two times the probe-interval for the SLA. Range: 60 to 7200.
cache disable	Selects cache option for the HTTP server. By default the option is enabled.
name-server {<IPV4-ADDR-DNS-SERVER> <IPV6-ADDR-DNS-SERVER>}	Specifies the DNS server for destination hostname resolution.
probe-interval <PROBE-INTERVAL>	Specifies the probe interval in seconds. Range: 30 to 604800.
proxy <PROXY-URL>	Specifies the probe interval in seconds. Range: 30 to 604800.

Parameter	Description
<code>source {<IPV4-ADDR> <IPV6-ADDR> IFNAME}</code>	Selects the source, either an IPv4 address, an IPv6 address, or hostname for SLA probes.
<code>source-port <SOURCE-PORT-NUM></code>	Specifies the value of the source port for the IP-SLA probes.
<code>version <VERSION-NUMBER></code>	Specifies the source interface to use for sending IP-SLA probes.
<code>http-raw-request <RAW-PAYLOAD></code>	Specifies the HTTP raw request. String.

Examples

Configuring HTTP get with parameters, including history interval:

```
switch(config)# ip-sla 1
switch(config-ipsla-1)# http get http://device.arubanetworks.com/root/home.html
history-interval 120 cache disable name-server 10.10.10.2 probe-interval 30
```

Configuring HTTP raw with parameters:

```
switch(config-ipsla-1)# http raw http://2.2.2.2 http-raw-request "GET
/en/US/hmpgs/index.html HTTP/1.0\r\n\r\n"
```

Disabling HTTP get with parameters:

```
switch(config-ipsla-1)# no http get http://device.example.com/root/home.html name-
server 10.10.10.2 history-interval 120
```

Disabling HTTP raw with parameters:

```
switch(config-ipsla-1)# no http raw http://device.example.com/root/home.html http-
raw-request "GET /en/US/hmpgs/index.html HTTP/1.0\r\n\r\n"
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added new parameter history-interval . Also, IPv6 addresses can be used.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla-<IP-SLA-NAME>	Administrators or local user group members with execution rights for this command.

https

```
https {get | raw} <URL> [history-interval <HISTORY-INTERVAL>] [cache disable] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}] [probe-interval <PROBE-INTERVAL>] [proxy <PROXY-URL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|IFNAME}] [source-port <SOURCE-PORT-NUM>] [version <VERSION-NUMBER>] [http-raw-request <RAW-PAYLOAD>]
```

```
no https {get | raw} <URL> [history-interval <HISTORY-INTERVAL>] [cache disable] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}] [probe-interval <PROBE-INTERVAL>] [proxy <PROXY-URL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|IFNAME}] [source-port <SOURCE-PORT-NUM>] [version <VERSION-NUMBER>] [http-raw-request <RAW-PAYLOAD>]
```

Description

Configures HTTPS as the IP-SLA test mechanism. Requires destination URL and type of HTTPS request (get/raw).

The **no** form of this command removes the configuration.



For HTTPS IP-SLA sessions, it is not required to install a certificate on the switch.

Parameter	Description
{get raw}	Selects HTTPS request type as get or raw where the system will generate or provide HTTPS payload.
<URL>	Specifies HTTPS URL address of syntax. https://<HOST NAME/IP-ADDRESS>:<PORT>/<PATH>.
history-interval <HISTORY-INTERVAL>	Configures the history interval for the IP-SLA. Set the history interval to minimum of two times the probe-interval for the SLA. Range: 60 to 7200.
cache disable	Selects cache option for the HTTPS server. By default the option is enabled.
name-server {<IPV4-ADDR-DNS-SERVER> <IPV6-ADDR-DNS-SERVER>}	Specifies the IPv4 address of DNS server.
probe-interval <PROBE-INTERVAL>	Specifies the probe interval in seconds. Range: 30 to 604800.
proxy <PROXY-URL>	Specifies the probe interval in

Parameter	Description
	seconds. Range: 30 to 604800.
<code>source {<IPV4-ADDR> <IPV6-ADDR> IFNAME}</code>	Selects the source, either an IPv4 address, an IPv6 address, or hostname for SLA probes.
<code>source-port <SOURCE-PORT-NUM></code>	Specifies the value of the source port for the IP-SLA probes.
<code>version <VERSION-NUMBER></code>	Specifies the source interface to use for sending IP-SLA probes.
<code>https-raw-request <RAW-PAYLOAD></code>	Specifies the HTTPS raw request. String.

Examples

Configuring HTTPS get with parameters:

```
switch(config-ipsla-1)# https get https://device.arubanetworks.com/root/home.html
```

Configuring HTTPS raw with parameters:

```
switch(config-ipsla-1)# https raw https://device.arubanetworks.com/root/home.html
raw-request "GET /en/US/hmpgs/index.html"
```

Removing the HTTPS raw:

```
switch(config-ipsla-1)# no https raw
https://device.arubanetworks.com/root/home.html raw-request "GET
/en/US/hmpgs/index.html"
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added new parameters history-interval . Also, IPv6 addresses can be used.
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla-<IP-SLA-NAME>	Administrators or local user group members with execution rights for this command.

icmp-echo

```
icmp-echo {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} [history-interval <HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>} [payload-size <PAYLOAD-SIZE>] [probe-interval <PROBE-INTERVAL>] [source {<SOURCE-IPV4-ADDR>|<SOURCE-IPV6-ADDR>|<IFNAME>}] [timeout <TIMEOUT>] [tos <TYPE-OF-SERVICE>]
```

```
no icmp-echo {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} [history-interval <HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>} [payload-size <PAYLOAD-SIZE>] [probe-interval <PROBE-INTERVAL>] [source {<SOURCE-IPV4-ADDR>|<SOURCE-IPV6-ADDR>|<IFNAME>}] [timeout <TIMEOUT>] [tos <TYPE-OF-SERVICE>]
```

Description

Configures ICMP echo as the IP-SLA test mechanism. Requires destination address for the IP-SLA test. The **no** form of this command disables the ICMP echo as the IP-SLA test mechanism.

Parameter	Description
{<DEST-IPV4-ADDR> <DEST-IPV6-ADDR> <HOSTNAME>}	Selects the destination, either an IPv4 address, an IPv6 address, or hostname, for the IP-SLA.
history-interval <HISTORY-INTERVAL>	Specifies the history interval for the IP-SLA. Set the history interval to minimum of two times the probe-interval for the SLA. Range: 10 to 7200.
name-server {<IPV4-ADDR-DNS-SERVER> <IPV6-ADDR-DNS-SERVER>}	Specifies the DNS server for destination hostname resolution.
payload-size <PAYLOAD-SIZE>	Specifies the payload size of an SLA probe. Range: 0 to 1440.
probe-interval <PROBE-INTERVAL>	Specifies the probe interval in seconds. Range: 5 to 604800.
source {<SOURCE-IPV4-ADDR> <SOURCE-IPV6-ADDR> <IFNAME>}	Selects the source IPv4 or IPv6 address for SLA probes or the source interface to use for sending IP-SLA probes.
timeout <TIMEOUT>	Specifies the interval before a probe is timed out. Range: 5 to 604800.
tos <TYPE-OF-SERVICE>	Specifies the type of serve value to be used in probe packets. Range: 0 to 255.

Examples

Configuring icmp-echo:

```
switch(config)# ip-sla test
switch(config-ip-sla-test)# icmp-echo 2.2.2.2 name-server 4.4.4.4 source 3.3.3.3
```

Configuring ICMP echo with several parameters, including history interval and timeout:

```
switch(config)# ip-sla test
switch(config-ip-sla-test)# icmp-echo 2.2.2.2 history-interval 160 name-server
4.4.4.4 payload-size 400 probe-interval 80 source 3.3.3.3 timeout 20 tos 255
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added two new parameters history-interval and timeout . Also, IPv6 addresses can be used.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla- <i><IP-SLA-NAME></i>	Administrators or local user group members with execution rights for this command.

ip-sla

```
ip-sla <IP-SLA-NAME>
no ip-sla <IP-SLA-NAME>
```

Description

Creates an IP Service Level Agreement (SLA) profile and switches to the **config-ip-sla** context.

The **no** form of this command deletes an IP-SLA profile. By default, all profile use the default VRF (default).

Parameter	Description
<i><IP-SLA-NAME></i>	Specifies an IP-SLA profile name. Length: 1 to 64 characters.

Examples

Creating an IP-SLA:

```
switch(config)# ip-sla 1
switch(config-ip-sla-1)#
```

Deleting an IP-SLA:

```
switch(config)# no ip-sla 1
switch(config)#
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ip-sla responder

```
ip-sla responder <SLA-NAME> (udp-echo | tcp-connect | udp-jitter-voip) [<PORT-NUM>]
[source {<SOURCE-IPV4-ADDR>|<SOURCE-IPV6-ADDR>|<IFNAME>}] [vrf <VRF-NAME>] [ipv6]
```

```
no ip-sla responder <SLA-NAME> (udp-echo | tcp-connect | udp-jitter-voip) [<PORT-NUM>]
[source {<SOURCE-IPV4-ADDR>|<SOURCE-IPV6-ADDR>|<IFNAME>}] [vrf <VRF-NAME>] [ipv6]
```

Description

Selects the IP-SLA responder. The responder can be configured for udp-echo, tcp-connect, udp-jitter-voip type. It requires the SLA name, SLA type, and port number as arguments.

The **no** form of this command removes the IP-SLA responder.

Parameter	Description
<SLA-NAME>	Specifies the IP-SLA responder name. Length: 1 to 64 characters.
udp-echo	Enables responder for udp-echo probes.
tcp-connect	Selects TCP connect as the IP-SLA test mechanism.
udp-jitter-voip	Selects VOIP jitter as the IP-SLA test mechanism.

Parameter	Description
<code><PORT-NUM></code>	Specifies the port number to listen for IP-SLA probes. Range: 1 to 65535.
<code>source {<SOURCE-IPV4-ADDR> <SOURCE-IPV6-ADDR> <IFNAME>}</code>	Selects the source IPv4 or IPv6 address for SLA probes or the source interface to use for sending IP-SLA probes.
<code>vrf <VRF-NAME></code>	Specifies the name of the VRF to use.
<code>ipv6</code>	Configures IPv6 responder. This keyword is required if an IPv6 address is being used by the source interface or VRF. By default, it will be considered as an IPv4 address.

Usage

The IPv6 keyword is required if an IPv6 address is being used by the source interface or VRF. Otherwise, by default, it will be considered as an IPv4 address.

Examples

Configuring IP-SLA responder for udp-echo:

```
switch(config)# ip-sla responder SLA1 udp-echo 8000 source 2.2.2.2
```

Configuring IP-SLA responder with IPv6:

```
switch(config)#ip-sla responder SLA1 udp-echo 8000 source 1/1/1 ipv6
```

Configuring IP-SLA responder for udp-jitter-voip:

```
switch(config)#ip-sla responder SLA1 udp-jitter-voip 1025 vrf <VRF>
```

Disabling IP-SLA responder:

```
switch(config)# no ip-sla responder SLA1 udp-echo 8000 source 2.2.2.2
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.15	Added ipv6 parameter.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show ip-sla all

show ip-sla all

Description

Shows all ip-sla source configuration and status.

Examples

Showing results for ip-sla all:

```
switch# show ip-sla all
SLA Name                : 2 (non-persistent)
Status                  : running
SLA Type                 : udp-echo
VRF                      : default
Source IP                :
Source Interface         :
Domain Name Server       :
Payload Size             : 28
TOS                      : 0
Probe Interval(seconds) : 60
History Interval(seconds) : 0
Timeout Interval(seconds) : 45

IP-SLA session status
IP-SLA Name              : 2 (non-persistent)
IP-SLA Type              : udp-echo
Destination Host Name/IP Address : 10.1.1.2
Destination Port          : 8888
Source IP Address/IFName :
Source Port              :
Status                   : running

IP-SLA Session Cumulative Counters
Total Probes Transmitted : 10
Probes Timed-out         : 10
Bind Error                : 0
Destination Address Unreachable : 0
DNS Resolution Failures  : 0
Reception Error           : 0
Transmission Error        : 0
Operational Status       : down

IP-SLA Latest Probe Results
Last Probe Time           :
Packets Sent              : 1
Packets Received          : 0
Packet Loss in Test       : 100%

Minimum RTT(ms)           :
Maximum RTT(ms)           :
```



```

Average RTT(ms) :
DNS RTT(ms) :

-----
SLA Name : echo-udp-sess2 (non-persistent)
Status : running
SLA Type : udp-echo
VRF : default
Source IP :
Source Interface :
Domain Name Server :
Payload Size : 28
TOS : 0
Probe Interval(seconds) : 60
History Interval(seconds) : 0
Timeout Interval(seconds) : 45

IP-SLA session status
IP-SLA Name : echo-udp-sess2 (non-persistent)
IP-SLA Type : udp-echo
Destination Host Name/IP Address : 100.1.1.2
Destination Port : 8888
Source IP Address/IFName :
Source Port :
Status : running

IP-SLA Session Cumulative Counters
Total Probes Transmitted : 10
Probes Timed-out : 0
Bind Error : 0
Destination Address Unreachable : 0
DNS Resolution Failures : 4
Reception Error : 0
Transmission Error : 0
Operational Status : Up

IP-SLA Latest Probe Results
Last Probe Time :
Packets Sent : 1
Packets Received : 1
Packet Loss in Test : 0.0000%

Minimum RTT(ms) :
Maximum RTT(ms) :
Average RTT(ms) :
DNS RTT(ms) :

-----

```

Showing results for non-configured ip-sla all:

```

switch# show ip-sla all
IPSLA source is not configured

```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Updated to display history interval .
10.12.1000	Updated to display https as an IP-SLA type.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip-sla responder

```
show ip-sla responder <SLA-NAME> [initiator {<SOURCE-IPV4-ADDR>|<SOURCE-IPV6-ADDR>}]
[<SOURCE-PORT-NUM>] [results]
```

Description

Shows the given IP-SLA responder configuration and operation status.

Parameter	Description
<SLA-NAME>	Specifies the SLA name.
initiator {<SOURCE-IPV4-ADDR> <SOURCE-IPV6-ADDR>}	Selects the source IPv4 or IPv6 address for SLA probes to use.
<SOURCE-PORT-NUM>	Configures the source port for the IP-SLA test. Range: 1 to 65535.
results	Displays the statistics for a given source IP and port.

Examples

Showing IP-SLA responder configuration:

```
switch# show ip-sla responder SLA3

SLA Name       : SLA3
IP-SLA Type    : Udp-echo
VRF            : Default
Responder Port  : 8000
Responder IP    : 2.2.2.3
Responder Interface : 1/1/1
Responder Status : Running
```

Showing IP-SLA responder with initiator and results parameters:

```
switch# show ip-sla responder SLA1 initiator 2.2.2.1 8000 results
```

```
IP-SLA Type      : Udp-echo
VRF Name         : Default
Source IP        : 2.2.2.1
Source Port      : 8000
Responder Port   : 8888
Responder IP     : 2.2.2.3
Responder Interface :
Responder Status : Running
Packets Received : 2
Packets Sent     : 2
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added new parameters: initiator and results .
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip-sla

```
show ip-sla <SLA-NAME> [{results | history-results}]
```

Description

Shows the given IP-SLA source configuration and status.

Parameter	Description
<SLA-NAME>	Specifies the SLA name.
results	Displays the statistics calculated for an SLA type.
history-results	Displays the history statistics calculated for the SLA ID.

Examples

Showing results for ip-sla:

```
switch# show ip-sla xyz results
IP-SLA session status
```

```

IP-SLA Name           : xyz
IP-SLA Type           : tcp-connect
Destination Host Name/IP Address: 2.2.2.1
Destination Port      : 8888
Source IP Address/IFName : 2.2.2.2
Source Port           : 5555
Status                : running

IP-SLA session cumulative counters
Total Probes Transmitted : 1
Probes Timed-out        : 0
Bind Error               : 0
Destination Address Unreachable : 0
DNS Resolution Failures : 0
Reception Error         : 0
Transmission Error      : 0

IP-SLA Latest Probe Results
Last Probe Time         : 2018 Jul 13 02:00:35
Packets Sent            : 1
Packets Received        : 1
Packet Loss in Test     : 0.0000%

Minimum RTT(ms)         : 12
Maximum RTT(ms)         : 12
Average RTT(ms)         : 12
DNS RTT(ms)             : 0
TCP RTT(ms)             : 12

```

Showing history results for ip-sla:

```

switch# sh ip-sla abcd history-results
IP-SLA Name: abcd

Session Details
=====
IP-SLA Type           : tcp-connect      Status                : running

Probe Interval(seconds) : 30              History Interval(seconds) : 600

Source Port           : 3000              Destination Port        : 4000

Source IP Address     : 10.0.0.1
Dest Host Name/IP Address : 10.0.0.2

History Probe Results
=====
Packet Stats
-----
Probes Transmitted    : 4              Packets Sent           : 4
Packets Received     : 4              Loss Percentage        : 0.0000%

Error Stats
-----
Transmission Errors  : 0              Reception Errors       : 0
Bind Errors          : 0              Dest. Unreachable     : 0
Probes Timed-Out     : 0              DNS Resolution Failures : 0

Probe RTT Stats

```

```

-----
Min  RTT (ms)          : 0          Max  RTT (ms)          : 0
Avg  RTT (ms)          : 0
DNS  RTT Stats
-----
Min  RTT (ms)          :             Max  RTT (ms)          :
Avg  RTT (ms)          :

```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added new parameter history-results . Updated to display history interval .
10.12.1000	Updated to display https as an IP-SLA type.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

start-test

start-test

Description

Starts the IP-SLA probes.

Examples

```

switch(config)# ip-sla test
switch(config-ip-sla-test)# start-test

```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla-<IP-SLA-NAME>	Administrators or local user group members with execution rights for this command.

stop-test

stop-test

Description

Stops the IP-SLA probes.

Examples

```
switch(config)# ip-sla test  
switch(config-ip-sla-test)# stop-test
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla-<IP-SLA-NAME>	Administrators or local user group members with execution rights for this command.

tcp-connect

```
tcp-connect {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} <DEST-PORT-NUM> [history-  
interval <HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}  
[probe-interval <PROBE-INTERVAL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|IFNAME}}] [source-port  
<PORT-NUM>]
```

```
no tcp-connect {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} <DEST-PORT-NUM> [history-  
interval <HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}  
[probe-interval <PROBE-INTERVAL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|IFNAME}}] [source-port  
<PORT-NUM>]
```

Description

Configures TCP connect as the IP-SLA test mechanism. Requires destination address/hostname and destination port for the IP-SLA of tcp-connect IP-SLA type.

The **no** form of this command removes the the TCP connection.

Parameter	Description
<code>{<DEST-IPV4-ADDR> <DEST-IPV6-ADDR> <HOSTNAME>}</code>	Selects the destination, either an IPv4 address, an IPv6 address, or hostname, for the IP-SLA.
<code><DEST-PORT-NUM></code>	Destination port for the IP-SLA. Range: 1 to 65535.
<code>history-interval <HISTORY-INTERVAL></code>	Configures the history interval for the IP-SLA. Set the history interval to minimum of two times the probe-interval for the SLA. Range: 60 to 7200.
<code>name-server {<IPV4-ADDR-DNS-SERVER> <IPV6-ADDR-DNS-SERVER>}</code>	Specifies the DNS server for destination hostname resolution.
<code>probe-interval <PROBE-INTERVAL></code>	Probe interval in seconds. Range: 30 to 604800.
<code>source {<IPV4-ADDR> <IPV6-ADDR> IFNAME>}</code>	Selects the source, either an IPv4 address, an IPv6 address, or hostname for SLA probes.
<code>source-port <PORT-NUM></code>	Specifies the port for the IP-SLA test.

Examples

Configuring TCP connect echo with parameters, including history interval:

```
switch(config)# ip-sla tcp
switch(config-ip-sla-tcp)# tcp-connect https://device.example.com 8080 name-server
10.10.10.2 history-interval 180 source 1/1/1 source-port 6000
```

Disabling the TCP connect:

```
switch(config-ip-sla-tcp)# no tcp-connect 10:1::1:1 8080 source 1/1/1 source-port
6000
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added new parameters history-interval . Also, IPv6 addresses can be used.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla-<IP-SLA-NAME>	Administrators or local user group members with execution rights for this command.

udp-echo

```
udp-echo {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} <DEST-PORT-NUM> [history-interval  
<HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}  
[payload-size <PAYLOAD-SIZE>] [probe-interval <PROBE-INTERVAL>] [source {<IPV4-  
ADDR>|<IPV6-ADDR>|IFNAME}}] [source-port <SOURCE-PORT-NUM>] [timeout <TIMEOUT>] [tos  
<TYPE-OF-SERVICE>]
```

```
no udp-echo {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} <DEST-PORT-NUM> [history-  
interval <HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}  
[payload-size <PAYLOAD-SIZE>] [probe-interval <PROBE-INTERVAL>] [source {<IPV4-  
ADDR>|<IPV6-ADDR>|IFNAME}}] [source-port <SOURCE-PORT-NUM>] [timeout <TIMEOUT>] [tos  
<TYPE-OF-SERVICE>]
```

Description

Configures UDP echo as the IP-SLA test mechanism. Requires destination address/hostname and destination port number for the IP-SLA of udp-echo SLA type.

The **no** form of this command removes the UDP echo configuration.

Parameter	Description
{<DEST-IPV4-ADDR> <DEST-IPV6-ADDR> <HOSTNAME>}	Selects the destination, either an IPv4 address, an IPv6 address, or hostname, for the IP-SLA.
<DEST-PORT-NUM>	Specifies the destination port for the IP-SLA. Range: 1 to 65535.
history-interval <HISTORY-INTERVAL>	Configures the history interval for the IP-SLA. Set the history interval to minimum of two times the probe-interval for the SLA. Range: 10 to 7200.
name-server {<IPV4-ADDR-DNS-SERVER> <IPV6-ADDR-DNS-SERVER>}	Specifies the DNS server for destination hostname resolution.
payload-size <PAYLOAD-SIZE>	Specifies the payload size of an SLA probe. Range: 28 to 1440.
probe-interval <PROBE-INTERVAL>	Specifies the probe interval in seconds. Range: 5 to 604800.
source {<IPV4-ADDR> <IPV6-ADDR> IFNAME>}	Selects the source, either an IPv4 address, an IPv6 address, or hostname for SLA probes.

Parameter	Description
<code>source-port <SOURCE-PORT-NUM></code>	Configures the source port for the IP-SLA test. Range: 1 to 65535.
<code>timeout <TIMEOUT></code>	Specifies the interval before a probe is timed out. Range: 5 to 604800.
<code>tos <TYPE-OF-SERVICE></code>	Specifies the type of service. Range: 0 to 255.

Examples

Configuring UDP echo with parameters, including history interval and timeout:

```
switch(config-ipsla-1)# udp-echo https://device.example.com 4000 history-interval
180 name-server 2.2.2.2 payload-size 100 probe-interval 90 source 4.4.4.4 source-
port 8000 timeout 20
```

Removing UDP echo configuration:

```
switch(config-ipsla-1)# no udp-echo https://device.example.com 8080 history-
interval 160 name-server 10.10.10.2 payload-size 50 source 2.2.2.1 timeout 20
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added two new parameters history-interval and timeout . Also, IPv6 addresses can be used.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ip-sla-<IP-SLA-NAME></code>	Administrators or local user group members with execution rights for this command.

udp-jitter-voip

```
udp-jitter-voip {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} <DEST-PORT-NUM>
[advantage-factor <ADVANTAGE-FACTOR>] [codec-type <CODEC-TYPE>] [history-interval
<HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}] [probe-
interval <PROBE-INTERVAL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|IFNAME}] [source-port
<SOURCE-PORT-NUM>] [tos <TYPE-OF-SERVICE>]
```

```
no udp-jitter-voip {<DEST-IPV4-ADDR>|<DEST-IPV6-ADDR>|<HOSTNAME>} <DEST-PORT-NUM>
[advantage-factor <ADVANTAGE-FACTOR>] [codec-type <CODEC-TYPE>] [history-interval
<HISTORY-INTERVAL>] [name-server {<IPV4-ADDR-DNS-SERVER>|<IPV6-ADDR-DNS-SERVER>}] [probe-
interval <PROBE-INTERVAL>] [source {<IPV4-ADDR>|<IPV6-ADDR>|IFNAME}] [source-port
<SOURCE-PORT-NUM>] [tos <TYPE-OF-SERVICE>]
```

Description

Configure UDP jitter VoIP as the IP-SLA test mechanism. Requires destination address/hostname and source address/interface for the IP-SLA of udp-jitter-voip IP-SLA type.

The **no** form of this command removes the UDP jitter VoIP configuration.

Parameter	Description
{<DEST-IPV4-ADDR> <DEST-IPV6-ADDR> <HOSTNAME>}	Selects the destination, either an IPv4 address, an IPv6 address, or hostname, for the IP-SLA.
<DEST-PORT-NUM>	Selects the port number for the IP-SLA. Range: 1 to 65535.
advantage-factor <ADVANTAGE-FACTOR>	Selects the value for the advantage factor. Default value is 0. Range: 0 to 20.
codec-type <CODEC-TYPE>	Selects the codec-type for the Voip IP-SLA test.
history-interval <HISTORY-INTERVAL>	Configures the history interval for the IP-SLA. Set the history interval to minimum of two times the probe-interval for the SLA. Range: 240 to 7200.
name-server {<IPV4-ADDR-DNS-SERVER> <IPV6-ADDR-DNS-SERVER>}	Specifies the DNS server for destination hostname resolution.
probe-interval <PROBE-INTERVAL>	Specifies the probe interval in seconds. Range: 120 to 604800.
source {<IPV4-ADDR> <IPV6-ADDR> IFNAME}	Selects the source, either an IPv4 address, an IPv6 address, or hostname for SLA probes.
source-port <SOURCE-PORT-NUM>	Specifies the value of source port for the IP-SLA probes.
tos <TYPE-OF-SERVICE>	Specifies the type of service. Range: 0 to 255.

Examples

Configuring udp-jitter-voip with optional parameters, including history interval:

```
switch(config-ipsla-1)# udp-jitter-voip https://device.arubanetworks.com 8080
advantage-factor 10 codec-type g711a history-interval 240 name-server 10.10.10.2
probe-interval 120 source 10.1.1.1 source-port 8888 tos 10
```

Configuring udp-jitter-voip with optional parameters:

```
switch(config-ipsla-1)# udp-jitter-voip 2.2.2.2 8080 advantage-factor 10 codec-
type g711a
```

Disabling udp-jitter-voip:

```
switch(config-ipsla-1)# no udp-jitter-voip https://device.example.com 8080
advantage-factor 10 codec-type g711a name-server 10.10.10.2 probe-interval 120
source 10.1.1.1 source-port 8888 tos 10
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.16.1000	Added new parameters history-interval . Also, IPv6 addresses can be used.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla- <i><IP-SLA-NAME></i>	Administrators or local user group members with execution rights for this command.

vrf

```
vrf <VRF-NAME>
no vrf [<VRF-NAME>]
```

Description

Configures the VRF on which the SLA will send or receive packets. By default, the default VRF is used. The **no** form of the command removes VRF from SLA.

Parameter	Description
<VRF-NAME>	Specifies a VRF name. Length: Default: default. If no VRF name is specified, then the default VRF name will be taken.

Examples

```
switch(config-ip-sla-test)# vrf ipslasrc
```

```
switch(config-ip-sla-test)# no vrf
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-sla- <i><IP-SLA-NAME></i>	Administrators or local user group members with execution rights for this command.

description

description <DESC>
no description

Description

Associates a text description with an IP tunnel for identification purposes.
The **no** form of this command removes the description from an IP tunnel.

Parameter	Description
<DESC>	Specifies the descriptive text to associate with the IP tunnel. Range: 1 to 64 printable ASCII characters.

Examples

Defines a description for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if) # description Network A Tunnel C
```

Removes the description for GRE tunnel **33**.

```
switch(config)# interface tunnel 33
switch(config-gre-if) # no description
```

Defines a description for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if) # description Network 3 Tunnel 27
```

Removes the description for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27
switch(config-ip-if) # no description
```

Defines a description for IPv6 in IPv6 tunnel **8**.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if) # description Network 4 Tunnel 8
```

Removes the description for IPv6 in IPv6 tunnel **8**.

```
switch(config)# interface tunnel 8
switch(config-if)# no description
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

destination ip

```
destination ip <IPv4-ADDR>
no destination ip <IPv4-ADDR>
```

Description

Sets the destination IP address for an IP tunnel. Specify the address of the interface on the remote device to which the tunnel will be established.

The **no** form of this command deletes the destination IP address from an IP tunnel.

Parameter	Description
<IPv4-ADDR>	Specifies the destination IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Defines the destination IP address to be **10.10.10.1** for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# destination ip 10.10.10.1
```

Deletes the destination IP address **10.10.10.1** from GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# no destination ip 10.10.10.1
```

Defines the destination IP address to be **10.10.20.1** for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-if)# destination ip 10.10.20.1
```

Deletes the destination IP address **10.10.20.1** from IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27
switch(config-if)# no destination ip 10.10.20.1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

destination ipv6

```
destination ipv6 <IPv6-ADDR>
no destination ipv6 [IPv6-ADDR]
```

Description

Sets the destination IPv6 address for an IP tunnel. Specify the address of the interface on the remote device to which the tunnel will be established.

The **no** form of this command deletes the destination IPv6 address from an IP tunnel.

Parameter	Description
<IPv6-ADDR>	Specifies the tunnel IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. This is optional in the no form of the command.

Examples

Defines the destination IPv6 address to be **2001:DB8::1** for IPv6 in IPv6 tunnel

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-if)# destination ipv6 2001:DB8::1
```

Deletes the destination IPv6 address **2001:DB8::1** from IPv6 in IPv6 tunnel **8**.

```
switch(config)# interface tunnel 8
switch(config-if)# no destination ipv6 2001:DB8::1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-if	Administrators or local user group members with execution rights for this command.

interface tunnel

```
interface tunnel <TUNNEL-NUMBER> mode {gre ip | ip 6in4 | ip 6in6 | ipsec ipv4}
interface tunnel <EXISTING-TUNNEL-NUMBER>
no interface tunnel <EXISTING-TUNNEL-NUMBER> [mode {gre ipv4 | ip 6in4 | ip 6in6}]
```

Description

Creates or updates an IP tunnel. After you enter the command, the firmware switches to the configuration context for the tunnel.

If the specified tunnel exists, this command switches to the context for the tunnel.

By default, all tunnels are automatically assigned to the default VRF when they are created.

The **no** form of this command deletes an existing IP tunnel. It is optional to include a mode in the **no** form, but if a mode has been entered, selecting a mode is required.



The option **ipv4** is deprecated and it is advised to use **ip** instead. Execute **show deprecated-commands** to view a list of deprecated commands.

Parameter	Description
mode {gre ip ip 6in4 ip 6in6}	Creates an IP tunnel. Choose one of the following options: ▪ gre ip: Creates a GRE tunnel. ▪ ip 6in4: Creates an IPv4 tunnel for IPv6 traffic. ▪ ip 6in6: Creates an IPv6 tunnel for IPv6 traffic. This is optional in the no form, unless a mode has already been entered.
<TUNNEL-NUMBER>	Specifies the number for a new tunnel. Range for 8100, 8320, 8325, 8325H, 8360, 9300, and 9300S switches: 1-255.

Parameter	Description
	Numbering is shared between all tunnels, so the same tunnel number cannot be used for an IPv6 in IPv4 tunnel and a GRE tunnel. Maximum number of GRE, 6in4 or 6in6 tunnels supported simultaneously for the 8320, 8325, 8325H, 8360, 9300, 9300S, and 10000 switch is 127.
<code><EXISTING-TUNNEL-NUMBER></code>	Specifies the number for an existing IP tunnel. Range for 8100, 8320, 8325, 8325H, 8360, 9300, and 9300S switches: 1-255. Numbering is shared between all tunnels, so the same tunnel number cannot be used for an IPv6 in IPv4 tunnel and a GRE tunnel. Maximum number of GRE, 6in4 or 6in6 tunnels supported simultaneously for the 8320, 8325, 8325H, 8360, 9300, 9300S, and 10000 switch is 127.

Examples

Defines a new GRE tunnel with number **27**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)#
```

Switches to the **config-gre-if** context for existing tunnel **33**.

```
switch(config)# interface tunnel 33
switch(config-gre-if)#
```

Deletes GRE tunnel **33**.

```
switch(config)# no interface tunnel 33
```

Defines a new IPv6 in IPv4 tunnel with number **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)#
```

Switches to the `config-ip-if` context for existing tunnel **27**.

```
switch(config)# interface tunnel 27
switch(config-ip-if)#
```

Deletes IPv6 in IPv4 tunnel **27**.

```
switch(config)# no interface tunnel 27
```

Defines a new IPv6 in IPv6 tunnel with number **8**.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-if)#
```

Deletes IPv6 in IPv6 tunnel with number **3**.

```
switch(config)# no interface tunnel 33 mode gre ipv4
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	The ipv4 parameter is deprecated and replaced with ip .
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if config	Administrators or local user group members with execution rights for this command.

ip address

```
ip address <IPv4-ADDR>/<MASK>
no ip address <IPv4-ADDR>/<MASK>
```

Description

Sets the local IP address of a GRE tunnel. This address identifies the tunnel interface for routing. It must be on the same subnet as the tunnel address assigned on the remote device.

The **no** form of this command deletes the local IP address assigned to a GRE tunnel.

Parameter	Description
<IPv4-ADDR>	Specifies the tunnel IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100 .
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.

Examples

Defines the local IP address **10.10.10.1** for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ip address 10.10.10.1/24
```

Deletes the local IP address **10.10.10.1** for GRE tunnel 33.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no ip address 10.10.10.1/24
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if	Administrators or local user group members with execution rights for this command.

ipv6 address

```
ipv6 address <IPV6-ADDR>/<MASK>
no ipv6 address <IPV6-ADDR>/<MASK>
```

Description

Sets the local IP address of an IPv6 to IPv4 tunnel or of an IPv6 to IPv6 tunnel. This address identifies the tunnel interface for routing. It must be on the same subnet as the tunnel address assigned on the remote device.

The **no** form of this command deletes the local IP address assigned to an IPv6 to IPv4 tunnel.

Parameter	Description
<IPV6-ADDR>	Specifies the tunnel IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.

Examples

Defines the local IP address **2001:DB8:5::1/64** for tunnel **8** for an IPv6 to IPv6 tunnel.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-if)# ipv6 address 2001:DB8:5::1/64
```

Deletes the local IP address **2001:DB8::1/32** for tunnel 8.

```
switch(config)# interface tunnel 8
switch(config-if)# no ipv6 address 2001:DB8:5::1/64
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-if config-if	Administrators or local user group members with execution rights for this command.

ip mtu

ip mtu <VALUE>

Description

Sets the MTU (maximum transmission unit) for an IP interface. The default value is 1500 bytes. The **no** form of this command sets the MTU to the default value of 1500 bytes.

Parameter	Description
<VALUE>	Specifies the MTU in bytes. Range: 1,280 bytes to 9,192 bytes.

Usage

The IP MTU is the largest IP packet that can be sent or received by the interface. For a tunnel, the IP MTU is the maximum size of the IP payload. To enable jumbo packet forwarding through the tunnel, set the IP MTU of the tunnel to a value greater than 1500. Also set the MTU and the IP MTU values for the underlying physical interface that the tunnel is using to a value greater than 1,500 bytes. The IP MTU of the tunnel must also be greater than or equal to the MTU of the ingress interface on the switch. The IP MTU value of the tunnel must also be less than or equal to the IP MT of the underlying interface that the tunnel is using.

When defining a GRE tunnel, the MTU has to account for 28 bytes of IP layer overhead, plus a GRE header. It must be larger than the MTU of the interface that the tunnel is using. Packets larger than the MTU are dropped.

Examples

Sets the MTU on GRE interface **33** to **1300** bytes.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# mtu 1300
```

Sets the MTU on GRE interface **33** to the default value.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ip mtu
```

Sets the MTU on IPv6 in IPv4 tunnel **27** to **1000** bytes.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# mtu 1000
```

Sets the MTU on IPv6 in IPv4 tunnel **27** to the default value.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# ip mtu
```

Sets the MTU on IPv6 in IPv6 tunnel **8** to **900** bytes.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# ip mtu 9000
```

Sets the MTU on IPv6 in IPv6 tunnel **8** to the default value.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# ip mtu
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

show interface tunnel

```
show interface tunnel[<TUNNEL-NUMBER>] [vsx-peer]
```

Description

Shows configuration settings for all IP tunnels, or a specific tunnel.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Shows configuration settings for tunnel **10**, which is a GRE tunnel in the following example.

```
switch# show interface tunnel10

Interface tunnel10 is up
Admin state is up
tunnel type GRE IP
tunnel interface IP address 192.0.2.0/24
tunnel source IP address 1.1.1.1
tunnel destination IP address 2.2.2.2
tunnel ttl 60
tunnel transport vrf red
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0

Shows configuration settings for tunnel **12**, which is an IPv6 in IPv6 tunnel in the following example.

```
switch# show interface tunnel12

Interface tunnel12 is up
Admin state is up
tunnel type IPv6 in IPv6
tunnel interface IPv6 address 4::1/64
tunnel source IPv6 address 2::1
tunnel destination IPv6 address 2::2
tunnel ttl 60
Description: Network2 Tunnel
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0

Shows configuration settings for all tunnels.

```
switch# show interface tunnel

Interface tunnel10 is up
Admin state is up
```

```
tunnel type GRE IP
tunnel interface IP address 192.0.2.0/24
tunnel source IP address 1.1.1.1
tunnel destination IP address 2.2.2.2
tunnel ttl 60
tunnel transport vrf BLue
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0

```
Interface tunnel11 is up
Admin state is up
tunnel type IPv6 in IPv4
tunnel source IPv4 address 198.51.100.0
tunnel destination IPv4 address 198.51.200.5
tunnel ttl 80
Description: Network11
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0

```
Interface tunnel12 is up
Admin state is up
tunnel type IPv6 in IPv6
tunnel interface IPv6 address 4::1/64
tunnel source IPv6 address 2::1
tunnel destination IPv6 address 2::2
tunnel ttl 60
Description: Network2 Tunnel
```

Statistics	RX	TX	Total
L3 Packets	0	0	0
L3 Bytes	0	0	0



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config interface tunnel

```
show running-config interface tunnel<TUNNEL-NUMBER> [vsx-peer]
```

Description

Shows the commands used to configure a tunnel.

Parameter	Description
<TUNNEL-NUMBER>	Specifies the number of an IP tunnel. Range: 1 to 127.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Shows the configuration for a GRE tunnel.

```
switch# show running-config interface tunnel2
interface tunnel 2 mode gre ipv4
source ip 10.10.20.11
destination ip 10.20.1.2
ip address 10.10.10.1/24
ttl 60
```

Shows the configuration for IPv6 in IPv4 tunnel.

```
switch# show running-config interface tunnel5
interface tunnel5 mode ip 6in4
source ip 10.10.10.12
destination ip 22.20.20.20
ip6 address 2001:DB8:5::1/64
ttl 60
no shutdown
description Network10
```

Shows the configuration for IPv6 in IPv6 tunnel.

```
switch# show running-config interface tunnel1
interface tunnel 1 mode ip 6in6
description Network2 Tunnel
source ipv6 2::1
destination ipv6 2::2
ipv6 address 4::1/64
ttl 60
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

shutdown

shutdown
no shutdown

Description

This command disables an IP interface. IP interfaces are disabled by default when created. The **no** form of this command enables an IP interface.

Examples

Enables GRE interface **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4  
switch(config-gre-if)# no shutdown
```

Disables GRE interface **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4  
switch(config-gre-if)# shutdown
```

Enables IPv6 in IPv4 interface **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4  
switch(config-ip-if)# no shutdown
```

Disables IPv6 in IPv4 interface **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4  
switch(config-ip-if)# shutdown
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-gre-if	Administrators or local user group members with execution rights for this command.
9300S	config-ip-if	

source ip

```
source ip <IPV4-ADDR>
no source ip <IPV4-ADDR>
```

Description

Sets the source IP address for an IP tunnel. Specify the IP address of a layer 3 interface on the switch. Tunnels can have the same source IP address and different destination IP addresses.

The **no** form of this command deletes the source IP address for an IP tunnel.

Parameter	Description
<IPV4-ADDR>	Specifies the source IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Defines the source IP address to be **10.10.20.1** for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# source ip 10.10.20.1
```

Deletes the source IP address **10.1.20.1** from GRE tunnel **33**.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no source ip 10.10.20.1
```

Defines the source IP address to be **10.10.10.1** for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# source ip 10.10.10.1
```

Deletes the source IP address **10.1.10.1** from IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no source ip 10.10.10.1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

source ipv6

```
source ipv6 <IPv6-ADDR>
no source ipv6 [IPv6-ADDR]
```

Description

Sets the source IPv6 address to be used for the encapsulation.

The **no** form of this command deletes the source IPv6 address for an IP tunnel.

Parameter	Description
<IPv6-ADDR>	Specifies the tunnel IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. This is optional in the no form of the command.

Examples

Defines the source IPv6 address to be **2001:DB8::1** for IPv6 in IPv6 tunnel **8**.

```
switch(config)# interface tunnel 8 mode ip 6in6
switch(config-ip-if)# source ipv6 2001:DB8::1
```

Deletes the source IP address **2001:DB8::1** from IPv6 in IPv6 tunnel **8**.

```
switch(config)# interface tunnel 8
switch(config-ip-if)# no source ipv6 2001:DB8::1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ip-if	Administrators or local user group members with execution rights for this command.

ttl

```
ttn <COUNT>
no ttn
```

Description

Sets the TTL (time-to-live), also known as the hop count, for tunneled packets. If not configured, the default value of 64 is used for the tunnel. (The hop count of the original packets is not changed.) A maximum of four different TTL values can be used at the same time by all tunnels on the switch. For example, if tunnel-1 has TTL 10, tunnel-2 has TTL 20, tunnel-3 has TTL 30, and tunnel-4 has TTL 40, then tunnel-5 cannot have a unique TTL value, it must reuse one of the values assigned to the other tunnels (10, 20, 30, 40).

The **no** form of this command sets TTL to the default value of 64.

Parameter	Description
<COUNT>	Specifies the hop count. Range: 1 to 255. Default: 64.

Examples

Defines a TTL of **99** for GRE tunnel **33**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# ttn 99
```

Sets the TTL for GRE tunnel **33** to the default value of 64.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no ttn
```

Defines a TTL of **55** for IPv6 in IPv4 tunnel **27**.

```
switch(config)# interface tunnel 27 mode ip 6in4
switch(config-ip-if)# ttn 55
```

Sets the TTL for IPv6 in IPv4 tunnel **27** to the default value of 64.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no ttn
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

vrf attach

```
vrf attach <VRF-NAME>
no vrf attach <VRF-NAME>
```

Description

Assigns an IP tunnel to a VRF. By default, all tunnels are automatically assigned to the default VRF when they are created.

The **no** form of this command assigns a tunnel to the default VRF (**default**).

Parameter	Description
<VRF-NAME>	Specifies the VRF name to which to assign the tunnel.

Examples

Assigns GRE tunnel **33** to **vrf1**.

```
switch(config)# interface tunnel 33 mode gre ipv4
switch(config-gre-if)# vrf attach vrf1
```

Reassigns GRE tunnel **33** to the default VRF.

```
switch(config)# interface tunnel 33
switch(config-gre-if)# no vrf attach vrf1
```

Assigns IPv6 in IPv4 tunnel **27** to **vrf2**.

```
switch(config)# interface tunnel 27 mode gre ipv4
switch(config-ip-if)# vrf attach vrf2
```

Reassigns IPv6 in IPv4 tunnel **27** to the default VRF.

```
switch(config)# interface tunnel 27
switch(config-ip-if)# no vrf attach vrf2
```

Assigns IPv6 in IPv6 tunnel **8** to **vrf3**.

```
switch(config)# interface tunnel 8 mode ip 6in6  
switch(config-ip-if) # vrf attach vrf3
```

Reassigns IPv6 in IPv6 tunnel **8** to the default VRF.

```
switch(config)# interface tunnel 8  
switch(config-ip-if) # no vrf attach vrf3
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-gre-if config-ip-if	Administrators or local user group members with execution rights for this command.

ip dhcp option ipv6-only-preferred

```
ip dhcp option ipv6-only-preferred
no ip dhcp option ipv6-only-preferred
```

Description

Enables the ipv6-only-preferred mode on the VLAN interface, and is also supported on the OOBM interface. Once enabled, the DHCP client prioritizes a IPv6 address over an IPv4 address. To obtain a DHCPv4 address, the **ipv6-only-preferred** command must be disabled, and the DHCPv4 client must be restarted. This command is disabled by default.



Ensure the server supports the ipv6-only-preferred mode option, as the command will not work unless supported by the server.

The **no** form of this command disables ipv6-only-preferred mode.



The ipv6-only-preferred mode command must be configured prior to the `ip dhcp` command, otherwise it will not take effect.

Parameter	Description
None	n/a

Examples

Enable the ipv6-only-preferred mode command:

```
switch(config-if-vlan)# ip dhcp option ipv6-only-preferred
```

Check the IPv6 only preferred configuration:

```
switch#(config)# show ip dhcp detail
DHCP Options: Broadcast-flag, Hostname

VRF default
-----
Interface vlan1
-----
IP address           : -
Default gateway      : -
Domain name          : -
DNS servers          :
Ipv6-only-preferred  : enabled
```

```

switch(config)#
switch(config-if-vlan)# show ipv6 dhcp

VRF default
-----
Interface vlan1
-----
IP address           : 3000::100/64
Domain search        : examplev6.org
DNS servers          : 3001::101, 2001::102
NTP servers          : 3000::201, 3012::202

switch(config-if-vlan)#

```

For the management interface, the config command is the same for ipv6-only-preferred mode, but the display command is different:

```

switch#(config)# interface mgmt
switch#(config-if-mgmt)# ip dhcp option
    ipv6-only-preferred Management interface ipv6-only-preferred option
    (Default:disabled)
switch(config-if-mgmt)# ip dhcp option ipv6-only-preferred
switch(config-if-mgmt)# show interface mgmt
Address Mode           : dhcp
Admin State            : up
Link State             : up
Mac Address            : 90:20:c2:1a:87:81
IPv4 address/subnet-mask :
Default gateway IPv4    :
IPv6 address/prefix     : 3000::240/64
IPv6 link local address/prefix : fe80::d8c4:e366:7903:5b16/64
Default gateway IPv6    : 3000::2/64
Primary Nameserver      : 3000::101
Secondary Nameserver    : 2000::102
Tertiary Nameserver     :
Ipv6-only-preferred     : Enabled
switch(config-if-mgmt)#

```

Disable the ipv6-only-preferred mode command:

```

switch(config-if-vlan)# no ip dhcp option ipv6-only-preferred

```

Command History

Release	Modification
10.16	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ipv6 address <global-unicast-address>

```
ipv6 address <global-unicast-address>
no ipv6 address <global-unicast-address>
```

Description

Sets a global unicast address on the interface.

The **no** form of this command removes the global unicast address on the interface.



This command automatically creates an IPv6 link-local address on the interface. However, it does not add the **ipv6 address link-local command** to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the **ipv6 address link-local** command.

Example

Enabling a global unicast address:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address 3731:54:65fe:2::a7
```

Disabling a global unicast address:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 address 3731:54:65fe:2::a7
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 address autoconfig

```
ipv6 address autoconfig
no ipv6 address autoconfig
```

Description

Enables the interface to automatically obtain an IPv6 address using router advertisement information and the EUI-64 identifier.

The **no** form of this command disables address auto-configuration.



- A maximum of 15 autoconfigured addresses are supported.
- This command automatically creates an IPv6 link-local address on the interface. However, it does not add the `ipv6 address link-local` command to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the `ipv6 address link-local` command.

Usage

The IPv6 SLAAC feature lets the router obtain the IPv6 address for the interface it is configured through the SLAAC method. This feature is not available on the `mgmt` VRF.

Example

Enabling unicast autoconfiguring:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address autoconfig
```

Disabling unicast autoconfiguring:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 address autoconfig
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 address link-local

`ipv6 address link-local [<IPV6-ADDR>/<MASK>]`

Description

Enables IPv6 on the current interface. If no address is specified, an IPv6 link-local address is auto-generated for the interface. If an address is specified, auto-configuration is disabled and the specified address/mask is assigned to the interface.

To disable IPv6 link-local on the interface, remove **ipv6 address link-local**, **ipv6 address <global-ipv6-address>**, and **ipv6 address autoconfig** from the interface.



This feature is not available on the management VRF.

Parameter	Description
<code><IPv6-ADDR></code>	Specifies the IP address in IPv6 format (<code>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</code>), where x is a hexadecimal number from 0 to F. You can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
<code><MASK></code>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Example

Enabling IPv6 link-local on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 address link-local
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 nd cache-limit

```
ipv6 nd cache-limit <CACHELIMIT>
no ipv6 nd cache-limit [<CACHELIMIT>]
```

Description

Configures the limit on the number of neighbor entries in the ND cache.

The **no** form of this command sets the cache limit to the default value.

Parameter	Description
<code><CACHELIMIT></code>	Specifies the neighbor cache entries limit. Range: 1-131072. Default: 131072.

Examples

Setting the cache limit to 20.

```
switch(config)# ipv6 nd cache-limit 20
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ipv6 nd dad attempts

```
ipv6 nd dad attempts <NUM-ATTEMPTS>  
no ipv6 nd dad attempts [<NUM-ATTEMPTS>]
```

Description

Configures the number of neighbor solicitations to be sent when performing duplicate address detection (DAD) for a unicast address configured on an interface. If the active gateway is configured with the same IP as an SVI IP, then IPv6 DAD cannot be configured.

The **no** form of this command sets the number of attempts to the default value.

Parameter	Description
<code>dad attempts <NUM-ATTEMPTS></code>	Specifies the number of neighbor solicitations to send. Range: 0-15. Default: 1.

Examples

```
switch(config)# interface 1/1/1  
switch(config-if)# ipv6 nd dad attempts 5
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd hop-limit

```
ipv6 nd hop-limit <HOPLIMIT>  
no ipv6 nd hop-limit [<HOPLIMIT>]
```

Description

Configures the hop limit to be sent in RAs.

The **no** form of this command resets the hop limit to 0. This reset eliminates the hop limit from the RAs that originate on the interface, so the host determines the hop limit.

Parameter	Description
hop-limit <HOPLIMIT>	Specifies the hop limit. Range: 0-255. Default: 64.

Examples

```
switch(config)# interface 1/1/1  
switch(config-if)# ipv6 nd hop-limit 64
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd mtu

```
ipv6 nd mtu <MTU-VALUE>
no ipv6 nd mtu [<MTU-VALUE>]
```

Description

Configures the MTU size to be sent in the RA messages.

The **no** form of this command sets hop limit to the default value.

Parameter	Description
<MTU-VALUE>	Specifies the MTU size. Range: 1280-65535 bytes. Default: 1500 bytes.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd mtu 1300
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ns-interval

```
ipv6 nd ns-interval <TIME>
no ipv6 nd ns-interval [<TIME>]
```

Description

Configures the ND time in milliseconds between DAD neighbor solicitations sent for an unresolved destination. Increase the ns-interval time if the network is slow or if there are persistent retry failures. If the active gateway is configured with the same IP as an SVI IP, then IPv6 DAD cannot be configured

The **no** form of this command sets the ns-interval to the default value.

Parameter	Description
<TIME>	Specifies the neighbor solicitation interval. Range: 1000-3600000 milliseconds. Default: 1000 milliseconds.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ns-interval 1200
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd prefix

```
ipv6 nd prefix <IPV6-ADDR>/<PREFIX-LEN>
    [no-advertise | [valid <LIFETIME-VALUE> preferred
    <LIFETIME-VALUE>] | no-autoconfig | no-onlink]

no ipv6 nd prefix <IPV6-ADDR>/<PREFIX-LEN> [no-advertise
    | [valid <LIFETIME-VALUE> preferred <LIFETIME-VALUE>
    ] | no-autoconfig | no-onlink]

ipv6 nd prefix default [no-advertise | [valid <LIFETIME-VALUE>
    preferred <LIFETIME-VALUE>] | no-autoconfig | no-onlink]}

no ipv6 nd prefix default [no-advertise | [valid <LIFETIME-VALUE>
    preferred <LIFETIME-VALUE>] | no-autoconfig | no-onlink]}
```

Description

Specifies prefixes for the routing switch to include in RAs transmitted on the interface. IPv6 hosts use the prefixes in RAs to autoconfigure themselves with global unicast addresses. The autoconfigured address of a host is composed of the advertised prefix and the interface identifier in the current link-local address of the host.

By default, advertise, autoconfig, and onlink are set.

The **no** form of this command removes the configuration on the interface.

Parameter	Description
<IPV6-ADDR>/<PREFIX-LEN>	Specifies the IPv6 prefix to advertise in RA. Format: X:X::X:X/M
default	Specifies apply configuration to all on-link prefixes that are not individually set by the ipv6 ra prefix <IPV6-ADDR>/<PREFIX-LEN> command. It applies the same valid and preferred lifetimes, link

Parameter	Description
	state, autoconfiguration state, and advertise options to the advertisements sent for all on-link prefixes that are not individually configured with a unique lifetime. This also applies to the prefixes for any global unicast addresses configured later on the same interface. Using default once, and then using it again with any new parameter values results in the new values replacing the former values in advertisements. If default is used without the no-advertise, no-autoconfig, or no-onlink parameter, the advertisement setting for the absent parameter is returned to its default setting.
no-advertise	Specifies do not advertise prefix in RA.
valid <LIFETIME-VALUE>	Specifies the total time, in seconds, the prefix remains available before becoming unusable. After preferred-lifetime expiration, any autoconfigured address is deprecated and used only for transactions only before preferred-lifetime expires. If the valid lifetime expires, the address becomes invalid. You can enter a value in seconds or enter valid infinite which sets infinite lifetime. Default: 2,592,000 seconds which is 30 days. Range: 0–4294967294 seconds.
preferred <LIFETIME-VALUE>	Specifies the span of time during which the address can be freely used as a source and destination for traffic. This setting must be less than or equal to the corresponding valid-lifetime setting. You can enter a value in seconds or enter preferred infinite which sets infinite lifetime. Default: 604,800 seconds which is seven days. Range: 0–4294967294 seconds.
no-autoconfig	Specifies do not use prefix for autoconfiguration.
no-onlink	Specifies do not use prefix for onlink determination.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd prefix 4001::1/64 valid 30 preferred 10 no-autoconfig
no-onlink
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra dns search-list

```
ipv6 nd ra dns search-list <DOMAIN-NAME> [lifetime <TIME>]
no ipv6 nd ra dns search-list <DOMAIN-NAME>
```

Description

Configures the DNS Search List (DNSSL) to include in Router Advertisements (RAs) transmitted on the interface.

The **no** form of this command removes the DNS Search List from the RAs transmitted on the interface.

Parameter	Description
<DOMAIN-NAME>	Specifies the domain names for DNS queries.
lifetime <TIME>	Specifies lifetime in seconds. Range: 4-4294967295 seconds. Default: 1800 seconds.

Usage

- DNSSL contains the domain names of DNS suffixes or IPv6 hosts to append to short, unqualified domain names for DNS queries.
- Multiple DNS domain names can be added to the DNSSL by using the command repeatedly.
- A maximum of eight server addresses are allowed.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns search-list test.com lifetime 500
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra dns server

```
ipv6 nd ra dns server <IPV6-ADDR> [lifetime <TIME>]
no ipv6 nd ra dns server <IPV6-ADDR>
```

Description

Configures the IPv6 address of a preferred Recursive DNS Server (RDNSS) to be included in Router Advertisements (RAs) transmitted on the interface.

The **no** form of this command removes the configured DNS server from the RAs transmitted on the interface.

Parameter	Description
<code><IPv6-ADDR></code>	Specifies the RDNSS address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. You can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
<code>lifetime <TIME></code>	Specifies IPv6 DNS server lifetime in seconds. Range: 4-4294967295 seconds. Default: 1800 seconds.

Usage

- Including RDNSS information in RAs provides DNS server configuration for connected IPv6 hosts without requiring DHCPv6.
- Multiple servers can be configured on the interface by using the command repeatedly.
- A maximum of eight server addresses are allowed.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns server 2001::1 lifetime 400
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra lifetime

```
ipv6 nd ra lifetime <TIME>
no ipv6 nd ra lifetime [<TIME>]
```

Description

Configures the lifetime, in seconds, for the routing switch to be used as a default router by hosts on the current interface.

The **no** form of this command sets lifetime to the default of 1800 seconds.

Parameter	Description
<code><TIME></code>	Specifies lifetime in seconds of a default router. A setting of 0 for default router lifetime in an RA indicates that the routing switch is not a default router on the interface. Range: 0-9000 seconds. Default: 1800 seconds.

Usage

- A given host on an interface refreshes the default router lifetime for a specific router each time the host receives an RA from that router.
- A specific router ceases to be a default router candidate for a given host if the default router lifetime expires before the host is updated with a new RA from the router.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra lifetime 1200
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra managed-config-flag

```
ipv6 nd ra managed-config-flag
no ipv6 nd ra managed-config-flag
```

Description

Controls the M flag setting in RAs the router transmits on the current interface. Enable the M flag to indicate that hosts can obtain IP address through DHCPv6. The M flag is disabled by default.

The **no** form of this command turns off (disables) the M flag.

Usage

- Enabling the M flag directs hosts to acquire their IPv6 addressing for the current interface from a DHCPv6 server.
- When the M-bit is enabled, receiving hosts ignore the O flag setting, which is configured using the command **ipv6 nd ra other-config-flag**.
- When the M-bit is disabled (the default), receiving hosts expect to receive their IPv6 addresses from RA.

M flag	O flag	Description
0	0	Indicates that no information is available via DHCPv6.
0	1	Indicates that other configuration information is available via DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.
1	0	Indicates that addresses are available via Dynamic Host Configuration Protocol (DHCPv6).
1	1	If the M flag is set, the O flag is redundant and can be ignored because DHCPv6 will return all available configuration information.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra managed-config-flag
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra max-interval

```
ipv6 nd ra max-interval <TIME>
no ipv6 nd ra max-interval [<TIME>]
```

Description

Configures the maximum interval between transmissions of IPv6 RAs on the interface. The interval between RA transmissions on an interface is a random value that changes every time an RA is sent. The interval is calculated to be a value between the current max-interval and min-interval settings. The **no** form of this command returns the setting to its default, provided the default value is less than the default lifetime value.

Parameter	Description
<i><TIME></i>	Specifies the maximum advertisement time in seconds. Range: 4-1800. Default: 600 seconds.

Usage

- This value has one setting per interface. The setting does not apply to RAs sent in response to a router solicitation received from another device.
- Attempting to set max-interval to a value that is not sufficiently larger than the current min-interval also results in an error message.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra max-interval 30
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra min-interval

```
ipv6 nd ra min-interval <TIME>
no ipv6 nd ra min-interval [<TIME>]
```

Description

Configures the minimum interval between transmissions of IPv6 RAs on the interface. The interval between RA transmissions on an interface is a random value that changes every time an RA is sent. The interval is calculated to be a value between the current max-interval and min-interval settings.

The **no** form of this command returns the setting to its default, provided the default value is less than the current max-interval setting.

Parameter	Description
<TIME>	Specifies a minimum advertisement time in seconds. Range: 3-1350. Default: 200 seconds.

Usage

- This value has one setting per interface and does not apply to RAs sent in response to a router solicitation received from another device.
- The min-interval must be less than the max-interval. Attempting to set min-interval to a higher value results in an error message.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra min-interval 25
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra other-config-flag

```
ipv6 nd ra other-config-flag
no ipv6 nd ra other-config-flag
```

Description

Controls the O-bit in RAs the router transmits on the current interface; but is ignored unless the M-bit is disabled in RAs. Configure to set the O-bit in RA messages for host to obtain network parameters through DHCPv6. The other-config-flag is disabled by default.

For more information on configuring the M-bit, see **ipv6 nd ra managed-config-flag**.

The **no** form of this command turns off (disables) the setting for this command in RAs.

Usage

Enabling the O-bit while the M-bit is disabled directs hosts on the interface to acquire their other configuration information from DHCPv6. Examples of such information are DNS-related information or information on other servers within the network.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra other-config-flag
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra reachable-time

```
ipv6 nd ra reachable-time <TIME>
no ipv6 nd ra reachable-time [<TIME>]
```

Description

Sets the amount of time that the interface considers a device to be reachable after receiving a reachability confirmation from the device.

The **no** form of this command sets the reachable time to the default value of 0. (no limit).

Parameter	Description
<TIME>	Specifies the reachable time in milliseconds. Range: 1000-3600000. Default: 0 (no limit).

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra reachable-time 2000
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd ra retrans-timer

```
ipv6 nd ra retrans-timer <TIME>
no ipv6 nd ra retrans-timer [<TIME>]
```

Description

Configures the period (retransmit timer) between ND solicitations sent by a host for an unresolved destination, or between DAD neighbor solicitation requests. By default, hosts on the interface use their own locally configured NS-interval settings instead of using the value received in the RAs. Increase this timer when neighbor solicitation retries or failures are occur, or in a "slow" (WAN) network. The **no** form of this command sets the value to the default of 0.

Parameter	Description
<TIME>	Specifies the retransmit timer value in milliseconds. Range: 0 - 4294967295 milliseconds. Default: 0 (Use locally configured NS-interval).

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra retrans-timer 400
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd route

```
ipv6 nd route <IPV6-ADDR>/<PREFIX-LEN> [no-advertise | lifetime {<SECONDS> | infinite} |
preference {low | medium | high}]
```



```
no ipv6 nd route <IPV6-ADDR>/<PREFIX-LEN> [no-advertise | lifetime {<SECONDS> | infinite}  
| preference {low | medium | high}]
```

Description

Configures the routing switch to include the routing information in the RAs transmitted on the interface. The routing switch includes the route information in the RA packets only if the configured routes are present in the routing table. After receiving the RA packets carrying the route information, the IPv6 host updates its routing table. The hosts lookup their routing table and selects the best possible route to forward packets.

The **no** form of this command removes the settings for including the routing information in the RA packets.

Parameter	Description
<IPV6-ADDR>/<PREFIX-LEN>	Specifies the IPv6 route prefix to advertise in RA. Format: X:X::X:X/M
no-advertise	Specifies to not advertise the route information.
lifetime {<SECONDS> infinite}	Specifies the duration in seconds that the route is valid for the route determination. If this parameter is configured with 0 , the route becomes invalid. Default: 1800 . Range: 0-4294967295 .
preference {low medium high}	Specifies the preference for the hosts to choose the router associated with the route over other routers when multiple identical route prefixes from different routers are received. Default: medium

Examples

Configuring routing information on interface **1/1/1**.

```
switch(config)# int 1/1/1  
switch(config-if)# ipv6 nd route 1::1/64 lifetime 200 preference high
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd router-preference

```
ipv6 nd router-preference {high | medium | low}
no ipv6 nd router-preference [high | medium | low]
```

Description

Specifies the value that is set in the Default Router Preference (DRP) field of Router Advertisements (RAs) that the switch sends from an interface. An interface with a DRP value of high will be preferred by other devices on the network over interfaces with an RA value of medium or low.

The **no** form of this command set the value to the default of medium.

Parameter	Description
high	Sets DRP to high.
medium	Sets DRP to medium. Default.
low	Sets DRP to low.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd router-preference high
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 nd suppress-ra

```
ipv6 nd suppress-ra [<SUPPRESS-OPTION>]
no ipv6 nd ra supress-ra [<SUPPRESS-OPTION>]
```

Description

Configures suppression of IPv6 Router Advertisement transmissions on an interface.

The **no** form of this command restores transmission of IPv6 Router Advertisement and options.

Parameter	Description
<code>suppress-ra</code> [<code><SUPPRESS-OPTION></code>]	Specifies suppressing RA transmissions. Entering <code>suppress-ra</code> without any options, suppresses all RA messages (default). Or you can enter one of the following options.
<code>dnssl</code>	Specifies suppressing DNSSL options in RA messages.
<code>mtu</code>	Specifies suppressing MTU options in RA messages.
<code>rdnss</code>	Specifies suppressing RDNSS options in RA messages.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd suppress-ra mtu dnssl rdnss
switch(config-if)# no ipv6 nd suppress-ra mtu dnssl rdnss
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Administrators or local user group members with execution rights for this command.

show ipv6 nd global traffic

`show ipv6 nd global traffic` [`vsx-peer`]

Description

Displays IPV6 Neighbor Discovery traffic details on a device.

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```

switch# show ipv6 nd global traffic
ICMPv6 packet Statistics (sent/received)
  Total Messages           :      18/0
  Error Messages           :       0/0
  Destination Unreachables :       0/0
  Time Exceeded            :       0/0
  Parameter Problems       :       0/0
  Echo Request             :       0/0
  Echo Replies             :       0/0
  Redirects                :       0/0
  Packet Too Big           :       0/0
  Router Advertisements    :       4/0
  Router Solicitations     :       0/0
  Neighbor Advertisements  :       0/0
  Neighbor Solicitations   :       3/0
  Duplicate router RA received :    0/0
ICMPv6 MLD Statistics (sent/received)
  V1 Queries :      0/0
  V2 Queries :      0/0
  V1 Reports  :      0/0
  V2 Reports  :     11/0
  V1 Leaves  :      0/0

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 nd interface

```
show ipv6 nd interface [<IF-NAME> | all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Displays neighbor discovery information for an interface. If no options are specified, displays information for the default VRF.

Parameter	Description
<IF-NAME>	Displays information about the specified IPv6 enabled interface.
all-vrfs	Displays information about interfaces in all VRFs.

Parameter	Description
vrf <VRF-NAME>	Displays information about interfaces in a particular VRF. Or, if <VRF-NAME> is not specified, information for the default VRF is displayed.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Two examples showing information for all VRFs:

```
switch# show ipv6 nd interface all-vrfs

List of IPv6 Interfaces for VRF default
Interface 1/1/1 is up
  Admin state is up
  IPv6 address:
  IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
  ICMPv6 active timers:
    Last Router-Advertisement sent:
    Next Router-Advertisement sent in:
  Router-Advertisement parameters:
    Periodic interval: 200 to 600 secs
    Router Preference: medium
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1800
    Send "Reachable Time" field: 0
    Send "Retrans Timer" field: 0
    Suppress RA: true
    Suppress MTU in RA: true
  ICMPv6 error message parameters:
    Send redirects: false
  ICMPv6 DAD parameters:
    Current DAD attempt: 1

List of IPv6 Interfaces for VRF red
Interface 1/1/2 is up
  Admin state is up
  IPv6 address:
    2001::1/64 [VALID]
  IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
  ICMPv6 active timers:
    Last Router-Advertisement sent:
    Next Router-Advertisement sent in:
  Router-Advertisement parameters:
    Periodic interval: 200 to 600 secs
    Router Preference: medium
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1800
    Send "Reachable Time" field: 0
```

```
Send "Retrans Timer" field: 0
Suppress RA: true
Suppress MTU in RA: true
ICMPv6 error message parameters:
Send redirects: false
ICMPv6 DAD parameters:
Current DAD attempt: 1
```

```
switch# show ipv6 nd interface all-vrfs
```

```
List of IPv6 Interfaces for VRF default
Interface vlan2 is up
Admin state is up
IPv6 address:
IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent:
  Next Router-Advertisement sent in:
Router-Advertisement parameters:
  Periodic interval: 200 to 600 secs
  Router Preference: medium
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1
```

```
List of IPv6 Interfaces for VRF red
Interface vlan3 is up
Admin state is up
IPv6 address:
  2001::1/64 [VALID]
IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent:
  Next Router-Advertisement sent in:
Router-Advertisement parameters:
  Periodic interval: 200 to 600 secs
  Router Preference: medium
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1
```

Showing information for interface 1/1/1:

```
switch# show ipv6 nd interface 1/1/1
Interface 1/1/1 is up
Admin state is up
IPv6 address:
IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent:
  Next Router-Advertisement sent in:
Router-Advertisement parameters:
  Periodic interval: 200 to 600 secs
  Router Preference: high
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1
```

```
switch# show ipv6 nd interface vlan 2
Interface vlan2 is up
Admin state is up
IPv6 address:
IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent:
  Next Router-Advertisement sent in:
Router-Advertisement parameters:
  Periodic interval: 200 to 600 secs
  Router Preference: high
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1
```

Showing information for the default VRF:

```
switch# show ipv6 nd interface

List of IPv6 Interfaces for VRF default
Interface 1/1/1 is up
Admin state is up
```

```

IPv6 address:
  2001::1/64 [VALID]
IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
ICMPv6 active timers:
  Last Router-Advertisement sent: 6 Secs
  Next Router-Advertisement sent in: 7 Secs
Router-Advertisement parameters:
  Periodic interval: 3 to 13 secs
  Router Preference: medium
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1900
  Send "Reachable Time" field: 0
  Send "Retrans Timer" field: 0
  Suppress RA: true
  Suppress MTU in RA: true
ICMPv6 error message parameters:
  Send redirects: false
ICMPv6 DAD parameters:
  Current DAD attempt: 1

```

```
switch# show ipv6 nd interface
```

```

List of IPv6 Interfaces for VRF default
Interface vlan2 is up
  Admin state is up
  IPv6 address:
    2001::1/64 [VALID]
  IPv6 link-local address: fe80::7272:cfff:fee7:a8b9/64 [VALID]
  ICMPv6 active timers:
    Last Router-Advertisement sent: 6 Secs
    Next Router-Advertisement sent in: 7 Secs
  Router-Advertisement parameters:
    Periodic interval: 3 to 13 secs
    Router Preference: medium
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1900
    Send "Reachable Time" field: 0
    Send "Retrans Timer" field: 0
    Suppress RA: true
    Suppress MTU in RA: true
  ICMPv6 error message parameters:
    Send redirects: false
  ICMPv6 DAD parameters:
    Current DAD attempt: 1

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 nd interface prefix

```
show ipv6 nd interface prefix [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows IPv6 prefix information for all VRFs or a specific VRF. If no options are specified, shows information for the default VRF.

Parameter	Description
all-vrfs	Shows prefix information for all VRFs.
vrf <VRF-NAME>	Name of a VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing prefix information for the default VRF:

```
switch# show ipv6 nd interface prefix

List of IPv6 Interfaces for VRF default
List of IPv6 Prefix advertised on 1/1/1
Prefix : 4545::/65
Enabled : Yes
Validlife time : 2592000
Preferred lifetime : 604800
On-link : Yes
Autonomous : Yes
```

```
switch# show ipv6 nd interface prefix

List of IPv6 Interfaces for VRF default
List of IPv6 Prefix advertised on vlan2
Prefix : 4545::/65
Enabled : Yes
Validlife time : 2592000
Preferred lifetime : 604800
On-link : Yes
Autonomous : Yes
```

Showing information for VRF red:

```
switch# show ipv6 nd interface prefix vrf red
```

```
List of IPv6 Interfaces for VRF red
List of IPv6 Prefix advertised on 1/1/2
  Prefix : 2001::/64
  Enabled : Yes
  Validlife time : 2592000
  Preferred lifetime : 604800
  On-link : Yes
  Autonomous : Yes
```

```
switch# show ipv6 nd interface prefix vrf red
```

```
List of IPv6 Interfaces for VRF red
List of IPv6 Prefix advertised on vlan3
  Prefix : 2001::/64
  Enabled : Yes
  Validlife time : 2592000
  Preferred lifetime : 604800
  On-link : Yes
  Autonomous : Yes
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 nd interface route

```
show ipv6 nd interface route [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays route information of all interfaces in the default VRF.

Parameter	Description
all-vrfs	Displays information about interfaces in all VRFs.
vrf <VRF-NAME>	Displays information about interfaces in a particular VRF. Or, if <VRF-NAME> is not specified, displays information for the default VRF.

Examples

Showing routing information for interface **1/1/1** in the default VRF:

```
switch# show ipv6 nd interface route

List of IPv6 Interfaces for VRF default
List of IPv6 Routes advertised on 1/1/1
Route : 1::/64
Enabled : Yes
Route lifetime : 200
Route preference : high
```

Showing routing information for interface **1/1/1** in VRF red:

```
switch# show ipv6 nd interface route vrf red

List of IPv6 Interfaces for VRF red
List of IPv6 Routes advertised on 1/1/2
Route : 2::/64
Enabled : No
Route lifetime : 1800
Route preference : low
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 nd ra dns search-list

```
show ipv6 nd ra dns search-list [vsx-peer]
```

Description

Displays domain name information on all interfaces.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns search-list test.com
switch# show ipv6 nd ra dns search-list
Recursive DNS Search List on: 1
    Suppress DNS Search List: Yes
    DNS Search 1: test.com    lifetime 1800
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 nd ra dns server

show ipv6 nd ra dns server [vsx-peer]

Description

Displays DNS server information on all interfaces.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 nd ra dns server 2001::1
switch# show ipv6 nd ra dns server
Recursive DNS Server List on: 1
    Suppress DNS Server List: Yes
    DNS Server 1: 2001::1    lifetime 1800
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

diag-dump irdp basic

diag-dump irdp basic

Description

Displays diagnostic information for IRDP.

Example

```
switch# diag-dump irdp basic
=====
[Start] Feature irdp Time : Thu Jun  8 09:50:28 2017
=====
-----
[Start] Daemon hpe-rdiscd
-----
Interface: 1/1/1 (state : Up)
rdisc ipv4 (enabled: 0, max:600, min:450, hold:1800, pref:0, isBcast:0)
Router IPs - 192.168.1.2,
Interface: 1/1/2 (state : Up)
rdisc ipv4 (enabled: 0, max:600, min:450, hold:1800, pref:0, isBcast:0)
Router IPs - 192.168.2.2,

-----
[End] Daemon hpe-rdiscd
-----
-----
[End] Feature irdp
=====
Diagnostic dump captured for feature irdp
```

```
switch# diag-dump irdp basic
=====
[Start] Feature irdp Time : Thu Jan  7 04:46:25 2021
=====
-----
[Start] Daemon hpe-rdiscd
-----
Interface: vlan2 (state : Down)
rdisc ipv4 (enabled: 1, max:600, min:450, hold:1800, pref:0, isBcast:0)
No advertisable IPv4 addresses on the interface
Interface: vlan1 (state : Down)
rdisc ipv4 (enabled: 0, max:600, min:450, hold:1800, pref:0, isBcast:0)
No advertisable IPv4 addresses on the interface

-----
[End] Daemon hpe-rdiscd
-----
```

```
=====
[End] Feature irdp
=====
Diagnostic-dump captured for feature irdp
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip irdp

```
ip irdp [broadcast | multicast]
no ip irdp
```

Description

Enables IRDP on an interface and specifies the packet type that is used to send advertisements. By default, the packet type is set to `multicast`. IRDP is only supported on layer 3 interfaces.

The **no** form of this command disables IRDP on an interface.

Parameter	Description
<code>broadcast</code>	Advertisements are sent as broadcast packets to IP address 255.255.255.255.
<code>multicast</code>	Advertisements are sent as multicast packets to the multicast group with IP address 24.0.0.1. Default.

Examples

Enabling IRDP on interface 1/1/1 with packet type set to the default value (multicast).

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp
```

Enabling IRDP on interface 1/1/1 with packet type set to broadcast.

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp broadcast
```

Disabling IRDP.

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip irdp holdtime

```
ip irdp holdtime <TIME>
no ip irdp holdtime <TIME>
```

Description

Specifies the maximum amount of time the host will consider an advertisement to be valid until a newer advertisement arrives. When a new advertisement arrives, hold time is reset. Hold time must be greater than or equal to the maximum advertisement interval. Therefore, if the hold time for an advertisement expires, the host can reasonably conclude that the router interface that sent the advertisement is no longer available. The default hold time is three times the maximum advertisement interval.

The **no** form of this command removes the specified maximum amount of time the host will consider an advertisement to be valid until a newer advertisement arrives and update it to the default value.

Parameter	Description
<TIME>	Specifies the lifetime of router advertisements sent from this interface. Range: 4 to 9000 seconds. Default: 1800 seconds.

Example

Setting the hold time for interface 1/1/1 to 5000 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp holdtime 5000
```


Removing the the hold time for interface 1/1/1 to 5000 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp holdtime 5000
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip irdp maxadvertinterval

```
ip irdp maxadvertinterval <TIME>
no ip irdp maxadvertinterval <TIME>
```

Description

Specifies the maximum router advertisement interval.

The **no** form of this command removes the specified maximum router advertisement interval and reverts to the default value.

Parameter	Description
<TIME>	Specifies the maximum time allowed between the sending of unsolicited router advertisements. Range: 4 to 1800 seconds. Default: 600 seconds.

Example

Setting the advertisement interval for interface 1/1/1 to 30 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp maxadvertinterval 30
```

Removing the advertisement interval for interface 1/1/1 to 30 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp maxadvertinterval 30
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip irdp minadvertinterval

```
ip irdp minadvertinterval <TIME>
no ip irdp minadvertinterval <TIME>
```

Description

Specifies the minimum amount of time the switch waits between sending router advertisements. By default, this value is automatically set by the switch to be 75% of the value configured for maximum router advertisement interval. Use this command to override the automatically configured value.

The **no** form of this command removes the specified minimum amount of time the switch waits between sending router advertisements and reverts to the default value.

Parameter	Description
<TIME>	Specifies the minimum time allowed between the sending of unsolicited router advertisements. Range: 3 to 1800 seconds. Default: 450 seconds (75% of the default value for maximum router advertisement interval).

Example

Setting the minimum advertisement interval for interface 1/1/1 to 25 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp minadvertinterval 25
```

Removing the minimum advertisement interval for interface 1/1/1 to 25 seconds:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp minadvertinterval 25
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip irdp preference

```
ip irdp preference <LEVEL>
no ip irdp preference <LEVEL>
```

Description

Specifies the IRDP preference level. If a host receives multiple router advertisement messages from different routers, the host selects the router that sent the message with the highest preference as the default gateway.

The **no** form of this command removes the specified IRDP preference level and reverts to the default value.

Parameter	Description
<LEVEL>	Specifies the IRDP preference level. Range: -2147483648 to 2147483647. Default: 0.

Example

Setting the IRDP preference level for interface 1/1/1 to 25.

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp preference 25
```

Removing the IRDP preference level for interface 1/1/1 to 25.

```
switch(config)# interface 1/1/1
switch(config-if)# no ip irdp preference 25
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

show ip irdp

```
show ip irdp [vsx-peer]
```

Description

Displays IRDP configuration settings.

Parameter	Description
<location>	Specifies one of these values: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.

vsx-peer

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show ip irdp
```

ICMP Router Discovery Protocol

Interface	Status	Advertising Address	Minimum Interval	Maximum Interval	Holdtime	Preference
1/1/1	Enabled	multicast	6	8	10	10
1/1/2	Disabled	multicast	450	600	1800	0
1/1/3	Enabled	broadcast	450	600	1800	115

```
switch# sh ip irdp
```

ICMP Router Discovery Protocol

Interface	Status	Advertising Address	Minimum Interval	Maximum Interval	Holdtime	Preference
vlan1	Disabled	multicast	450	600	1800	0
bridge_normal	Disabled	multicast	450	600	1800	0



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

address-family

```
address-family [<AFI> | <SAFI>] [ip | ipv6] [unicast]
[no] address-family <AFI> | <SAFI>
```

Description

Initializes the appropriate address-family and enters address-family configuration mode for IPv4 or IPv6. The unicast option is available to configure the subaddress family identifier.

The **no** form of the command removes the association of the specified address-family. The address-family specific routes that are leaked from this VRF will be withdrawn.

Parameter	Description
AFI	Required: Specifies address family identifier.
SAFI	Required: Specifies subaddress family identifier.
ip	Optional: IPv4 address family
ipv6	Optional: IPv6 address family
unicast	The subaddress family identifier. When the unicast option is used, the command context changes to config-vrf-af-ipv4-uc .

Examples

Address family command for IPv4 unicast:

```
switch(config-vrf)# address-family ipv4 unicast
switch(config-vrf)#no address-family ipv4 unicast
```

Address family command for IPv6 unicast:

```
switch(config-vrf)# address-family ipv6 unicast
switch(config-vrf)#no address-family ipv6 unicast
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	The ipv4 keyword is deprecated and replaced with ip .
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-vrf	Administrators or local user group members with execution rights for this command.

ip|ipv6 vrf

```
[ip|ipv6] route <PREFIX> <SRC-VRF-LOCAL-IFACE><SRC-VRF-NEXTHOP-IP> vrf <DST-VRF-NAME>
[name <WORD>]
no [ip|ipv6] route <PREFIX> <SRC-VRF-LOCAL-IFACE><SRC-VRF-NEXTHOP-IP> vrf <DST-VRF-NAME>
[name <WORD>]
```

Description

The IP/IPv6 route command sets the subnet mask, the reachable network interface, the next-hop IP for the reachable network, and the VRF route leak destination.

Parameter	Description
<PREFIX>	The subnet mask (prefix of the network).
<SRC-VRF-LOCAL-IFACE>	The interface which is reachable by the network.
<SRC-VRF-NEXTHOP-IP>	The next-hop IP for the reachable network.
<DST-VRF-NAME>	The VRF route leak destination.
name <WORD>	Assigns a name to the destination route. Range: 1 to 64 characters.

Examples

Using the command, leak the named route Blue VRF, using prefix 100.0.0.0/24 which is reachable by the next-hop IP 20.0.0.1 on the interface 1/1/1 from VRF Red:

```
switch(config)# ip route 100.0.0.0/24 1/1/1 20.0.0.1 vrf blue
```

Assign a name to the destination route:

```
switch(config)# ip route 20.0.4.0/24 10.0.0.2 vrf test name VRF-Management
```

The following example shows the route in the source VRF, the corresponding command executed in the other VRF, and howidcates how the routing tables is displayed after the command is executed.

```

switch(config)# show running-config
Current configuration:
!
vrf blue
vrf green
vrf red
!
vlan 1
interface 1/1/19
    no shutdown
    vrf attach red
    ip address 10.0.0.1/24
interface 1/1/20
    no shutdown
    vrf attach green
    ip address 20.0.0.1/24
interface 1/1/21
    no shutdown
    vrf attach blue
    ip address 40.0.0.1/24
interface 1/1/22
no shutdown

switch(config)# ip route 30.0.0.0/24 20.0.0.2 vrf green
switch(config)# ip route 50.0.0.0/24 20.0.0.2 vrf green
switch(config)# ip route 30.0.0.0/24 1/1/20 20.0.0.2 vrf red
switch(config)# ip route 50.0.0.0/24 1/1/20 20.0.0.2 vrf blue
switch(config)# ip route 40.0.0.0/24 1/1/21 vrf red

```

```
switch# show ip route vrf green
```

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local

R - RIP, B - BGP, O - OSPF, D - DHCP

Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN

IA - OSPF internal area, E1 - OSPF external type 1

E2 - OSPF external type 2

Flags: F - FIB-optimized route

VRF: green

Prefix (egress) Type	Origin/ Metric	Nexthop Distance/ Age	Interface	VRF

20.0.0.0/24	-		1/1/20	-
C	[0/0]	-		
20.0.0.1/32	-		1/1/20	-
L	[0/0]	-		
30.0.0.0/24	20.0.0.2		1/1/20	-
S	[1/0]	00h:05m:16s		
50.0.0.0/24	20.0.0.2		1/1/20	-
S	[1/0]	00h:05m:16s		

Total Route Count : 4

```
switch# show ip route vrf blue
```

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local

R - RIP, B - BGP, O - OSPF, D - DHCP

Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN

IA - OSPF internal area, E1 - OSPF external type 1

E2 - OSPF external type 2


```

Flags:          F - FIB-optimized route
VRF: blue
Prefix          Nexthop
(egress)        Origin/  Distance/  Age
Type           Metric
-----
40.0.0.0/24      -
                  C      [0/0]      -
40.0.0.1/32      -
                  L      [0/0]      -
50.0.0.0/24      20.0.0.2
                  S      [1/0]      00h:00m:44s
Total Route Count : 3

```

```

switch# show ip route vrf red
Displaying ipv4 routes selected for forwarding
Origin Codes: C - connected, S - static, L - local
R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
IA - OSPF internal area, E1 - OSPF external type 1
E2 - OSPF external type 2
Flags:          F - FIB-optimized route
VRF: red
Prefix          Nexthop
(egress)        Origin/  Distance/  Age
Type           Metric
-----
10.0.0.0/24      -
                  C      [0/0]      -
10.0.0.1/32      -
                  L      [0/0]      -
30.0.0.0/24      20.0.0.2
                  S      [1/0]      00h:00m:48s
40.0.0.0/24      -
                  S      [1/0]      00h:00m:48s
100.100.1.0/24    -
                  C      [0/0]      -
100.100.1.7/32    -
                  L      [0/0]      -
Total Route Count : 6

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	The name parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ipv6 route source interface

```
ipv6 route <IPv6 ADDR/MEMBER><IPv6 ADDR> source <INTERFACE>
[<DISTANCE> | <VRF INSTANCE-NAME>]
no ipv6 route
```

Description

Creates a route leak between the source VRF and destination VRF. Using the static method, the route must first be added to the destination VRF. The route is added to the local interface of the source VRF with a next-hop interface. The existing IPv6 route command takes the source interface only when next-hop IP is link-local. To support VRF route leaking for global IPv6 unicast addresses, the command takes next-hop interface information along with next-hop IP regardless of next-hop IP is link-local or not.

- Users must provide both the next-hop IP and the interface information to leak the global unicast IPv6 network routes (route that is not directly reachable).
- The next-hop IP information is not required to leak connected global unicast IPv6 routes (route that is directly reachable).

The **no** form of command deletes the static VRF leaked route.

Parameter	Description
<IPv6 ADDR/MEMBER>	Required: IPv6 IP-Address route destination.
<IPv6 ADDR>	Required: IPv6 route destination
<INTERFACE>	Required: The outgoing interface. Use the format member/slot/port (for example, 1/3/1).
<DISTANCE>	Optional: administrative distance of static route
<VRF INSTANCE-NAME>	Optional: VRF instance

Options

nullroute

Discard packets to the destined route silently.

reject

Discard packets to the destined route and return ICMP error to the sender.

Examples

Configures a route leak between the source VRF and destination VRF:

```
switch(config)# show runn
Current configuration:
!
```

```

vrf blue
    vrf green
vrf red
    !

vlan 1
    interface 1/1/1
    no shutdown
    vrf attach red
    ip address 2000::1/64
    interface 1/1/2
    no shutdown
    vrf attach green
    ip address 3000::1/64
    interface 1/1/3
    no shutdown
    vrf attach blue
    ip address 4000::1/64

switch(config)# ipv6 route 5000::0/64 3000::2 source 1/1/2 vrf red
switch(config)# ipv6 route 6000::0/64 3000::3 source 1/1/2 vrf blue

switch(config)# show runn
Current configuration:
!
vrf blue
    vrf green
vrf red
    !

vlan 1
    interface 1/1/1
    no shutdown
    vrf attach red
    ip address 2000::1/64
    interface 1/1/2
    no shutdown
    vrf attach green
    ip address 3000::1/64
    interface 1/1/3
    no shutdown
    vrf attach blue
    ip address 4000::1/64

    ipv6 route 5000::0/64 3000::2 source 1/1/2 vrf red
    ipv6 route 6000::0/64 3000::3 source 1/1/2 vrf blue

switch(config)# no ipv6 route 5000::0/64 3000::2 source 1/1/2 vrf red
switch(config)# no ipv6 route 6000::0/64 3000::3 source 1/1/2 vrf blue

switch(config)# show runn
Current configuration:
!
    vrf blue
    vrf green
vrf red
    !

    vlan 1
        interface 1/1/1

```

```

no shutdown
vrf attach red
    ip address 2000::1/64
    interface 1/1/2
    no shutdown
    vrf attach green
ip address 3000::1/64
    interface 1/1/3
    no shutdown
    vrf attach blue
    ip address 4000::1/64

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ip route interface

```

ip route <IPv4 ADDR/MEMBER> interface <IPv4 ADDR>
[<DISTANCE> | <VRF INSTANCE-NAME>]
no ip route

```

Description

Creates a route leak between the SRC-VRF and DST-VRF. Using the static method, the route must first be added to the destination VRF. The route is added to the local interface of the source VRF with a next-hop interface. The existing IP route command can then take either the next-hop IP or the next-hop interface.

- **INTERFACE** refers to the outgoing interface in an m/s/p format
- Users must provide both the next-hop IP and the interface information to leak network routes.
- The next-hop IP information is not required to leak connected routes.

The [no] form of command deletes the static VRF leaked route.

Parameter	Description
<IPv4 ADDR/MEMBER>	Required: IPv4 IP-Address route destination.

Parameter	Description
<IPv4 ADDR>	Required: IPv4 route destination
<DISTANCE>	Optional: administrative distance of static route
<VRF INSTANCE-NAME>	Optional: VRF instance

Options

nullroute

Discard packets to the destined route silently.

reject

Discard packets to the destined route and return ICMP error to the sender.

Example

Configures a route leak between the SRC-VRF and DST-VRF:

```
switch(config)# show runn
Current configuration:
!
vrf blue
    vrf green
vrf red
!

vlan 1
    interface 1/1/1
    no shutdown
        vrf attach red
    ip address 10.0.0.1/24
        interface 1/1/2
        no shutdown
        vrf attach green
    ip address 20.0.0.1/24
    interface 1/1/3
        no shutdown
        vrf attach blue
    ip address 40.0.0.1/24

switch(config)# ip route A.B.C.D/M IPv4 route destination
switch(config)# ip route A.B.C.D/M IPv4 route destination
switch(config)# ip route 30.0.0.0/24 A.B.C.D Nexthop IPv4 address
switch(config)# ip route 30.0.0.0/24 1/1/2 A.B.C.D Nexthop IPv4 address
switch(config)# ip route 30.0.0.0/24 20.0.0.2 vrf green
switch(config)# ip route 30.0.0.0/24 1/1/2 20.0.0.2 vrf red
switch(config)# ip route 50.0.0.0/24 1/1/2 20.0.0.2 vrf blue
switch(config)# ip route 50.0.0.0/24 20.0.0.2 vrf green
switch(config)# ip route 60.0.0.0/24 1/1/2 vrf red

switch(config)# show runn
Current configuration:
!
vrf blue
    vrf green
vrf red
!
```

```

vlan 1
  interface 1/1/1
  no shutdown
    vrf attach red
  ip address 10.0.0.1/24
    interface 1/1/2
    no shutdown
    vrf attach green
  ip address 20.0.0.1/24
  interface 1/1/3
    no shutdown
  vrf attach blue
  ip address 40.0.0.1/24
  ip route 30.0.0.0/24 1/1/2 20.0.0.2 vrf red
  ip route 50.0.0.0/24 1/1/2 20.0.0.3 vrf blue
  ip route 60.0.0.0/24 1/1/2 vrf red

switch(config)# no ip route 30.0.0.0/24 1/1/2 20.0.0.2 vrf red
switch(config)# no ip route 50.0.0.0/24 1/1/2 20.0.0.3 vrf blue
switch(config)# no ip route 60.0.0.0/24 1/1/2 vrf red

switch(config)# show runn
Current configuration:
!
  vrf blue
  vrf green
vrf red
!

vlan 1
  interface 1/1/1
  no shutdown
  vrf attach red
  ip address 10.0.0.1/24
  interface 1/1/2
  no shutdown
  vrf attach green
  ip address 20.0.0.1/24
  interface 1/1/3
  no shutdown
  vrf attach blue
  ip address 40.0.0.1/24

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

rd

```
rd <AS-NUMBER:NN>
no rd <AS-NUMBER:NN>
```

Description

Configures VRF table with specified route-distinguisher value. An RD ensures uniqueness of a route between multiple VRFs.

The **no** form of the command will delete RD from a specified VRF table. The VRF instance goes down when RD is deleted. All routes that are exported or leaked from the deleted VRF will be withdrawn.

Parameter	Description
<AS-NUMBER:NN>	Required: Enter an AS number and an arbitrary number.

Examples

Configures VRF for RD with an AS number 100:1.

```
switch(config-vrf) # rd 100:1
```

Deletes the RD from the specified VRF.

```
switch(config-vrf) # no rd
```

Deletes the RD and AS number from the specified VRF.

```
switch(config-vrf) # no rd 100:1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-vrf	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute <protocol> [route-map <route-map-name>]  
[no] redistribute <protocol> [route-map <route-map-name>]
```

Description

Specifies the protocol routes to redistribute to BGP VRF context. Any routes existing in the BGP VRF context are leaked as a VPNv4 or VPNv6 prefixes to other VRFs based on BGP route-targets.

The **no** form of this command removes the protocol.

Parameter	Description
<code>redistribute</code>	Required: redistributes routes from another routing protocol.
<code>connected</code>	Optional: redistribute directly attached networks.
<code>ospfv3</code>	Optional: redistributes OSPFv3 routes.
<code>static</code>	Optional: redistributes static routes.
<code>route-map</code>	Optional: applies route map policy for redistribution.

Examples

The following is an example of redistributing OSPFv2 routes to a BGP **vrf cust_a** instance by creating a router BGP instance for **cust_a**.

1. Creating the router BGP instance for **cust_a**.

```
switch(config)# router bgp 1  
switch(config-router) # vrf cust_a
```

2. Redistributing the router to BGP.

```
switch(config-router-bgp) # redistribute ospf
```

The following is an example of redistributing OSPFv3 routes to a BGP **vrf cust_a** instance by creating a router BGP instance for **cust_a**.

1. Creating the router BGP instance for **cust_a**

```
switch(config)# router bgp 100  
switch(config-router) # vrf cust_a
```

2. Configuring the address family IPv6 unicast to the router

```
switch(config-router-bgp) # address-family ipv6 unicast
```


3. Redistributing the router to OSPFv3

```
switch(config-router-ipv6-uc)# redistribute ospfv3
```

4. Redistributing the router configured with `ipv6-af-us` to OSPFv3

```
switch(config-router-bgp-vrf-ipv6-af-uc)# redistribute ospfv3
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

route-target

```
route-target [import | export | both] <AS-NUMBER:NN>  
no route-target [import | export | both] <AS-NUMBER:NN>
```

Description

BGP route targets are extended BGP communities that identify the VPNv4 or VPNv6 routes that are associated with a VRF. This command specifies the route targets used on the import or export of the routes to other VRFs. Multiple route targets can be associated with a VRF.

The **no** form of the command removes the association.

Parameter	Description
import	Specifies the RTs imported to the VRF. Import or export or both required Literal Specifies the route-target type.
export	Specifies the RT on VPNv4 or VPNv6 prefixes that are leaked to other VRFs.
both	Specifies the RT for both export and import types.
<AS-NUMBER:NN>	Specifies an AS number and an arbitrary number for the RT value.

Examples

Configuring route targets for several VRFs.

```

switch(config)# vrf default
switch(config-vrf)# rd 192.168.2.1:0
switch(config-vrf)# address-family ipv4 unicast
switch(config-vrf-ipv4-af-uc)# route-target export 65001:0
switch(config-vrf-ipv4-af-uc)# route-target import 65001:1
switch(config-vrf-ipv4-af-uc)# route-target import 65001:2
switch(config-vrf-ipv4-af-uc)# exit-address-family
switch(config-vrf)# exit
switch(config)# vrf VRF1
switch(config-vrf)# rd 192.168.2.1:1
switch(config-vrf)# address-family ipv4 unicast
switch(config-vrf-ipv4-af-uc)# route-target export 65001:1
switch(config-vrf-ipv4-af-uc)# route-target import 65001:0
switch(config-vrf-ipv4-af-uc)# exit-address-family
switch(config-vrf)# exit
switch(config)# vrf VRF2
switch(config-vrf)# rd 192.168.2.1:2
switch(config-vrf)# address-family ipv4 unicast
switch(config-vrf-ipv4-af-uc)# route-target export 65001:2
switch(config-vrf-ipv4-af-uc)# route-target import 65001:0
switch(config-vrf-ipv4-af-uc)# exit-address-family
switch(config-vrf)# exit

```

Configuring the route target for export. Removing the configuration for export.

```

switch(config-vrf-ipv4-af-uc)# route-target export 100:1
switch(config-vrf-ipv4-af-uc)# no route-target export 100:1

```

Configuring the route target for import. Removing the configuration for import.

```

switch(config-vrf-ipv4-af-uc)# route-target import 100:2
switch(config-vrf-ipv4-af-uc)# no route-target import 100:2

```

Configuring the route target for both import and export. Removing the configuration for import and export.

```

switch(config-vrf-ipv4-af-uc)# route-target both 100:3
switch(config-vrf-ipv4-af-uc)# no route-target both 100:3

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

route-target export

```
route-target export route-map <ROUTE-MAP-NAME>
no route-target export route-map <ROUTE-MAP-NAME>
```

Description

This command specifies the route-map to be used while exporting routes to VRF. Route target export route-map is configured to filter the routes those are leaked to VRF.

The **no** form of the command removes the specification.

Parameter	Description
route-map	Specifies route-map policy for export.
<ROUTE-MAP-NAME>	Specifies route-map policy name



VPNv4 SAFI is not supported.

Examples

Configuring route-map for route target export in IPv4:

```
switch(config)# vrf cust_a
switch(config-vrf)# address-family ipv4 unicast
switch(config-vrf-ipv4-af-uc)# route-target export route-map rmap
```

Removing the configuration for export in IPv4:

```
switch(config)# vrf cust_a
switch(config-vrf)# address-family ipv4 unicast
switch(config-vrf-ipv4-af-uc)# no route-target export route-map rmap
```

Configuring route-map for route target export in IPv6:

```
switch(config)# vrf cust_a
switch(config-vrf)# address-family ipv6 unicast
switch(config-vrf-ipv6-af-uc)# route-target export route-map rmap
```

Removing the configuration for export in IPv6:

```
switch(config)# vrf cust_a
switch(config-vrf)# address-family ipv6 unicast
switch(config-vrf-ipv6-af-uc)# no route-target export route-map rmap
```

Match prefix-list and set metric is only supported for route-target export route-map:

```
route-map rmap permit seq 1
  match ip address prefix-list prefix
```

```
set metric 400
ip prefix-list seq 1 permit 14.1.1.0/24
```



Applies to both IPv4 and IPv6 address family only.

Only one route-target export route-map per VRF can be configured.



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-vrf	Administrators or local user group members with execution rights for this command.

router bgp

```
router bgp <AS-NUMBER>
no router bgp <AS-NUMBER>
```

Description

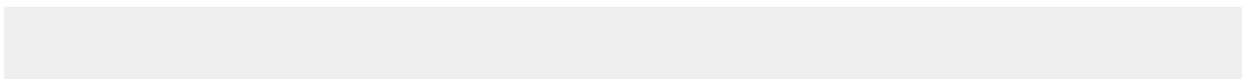
This command configures the BGP instance on the router, configures the AS (Autonomous System) the router belongs to, and enters into the BGP router configuration mode. Only a single BGP AS number can be assigned for the entire system.

The **no** form of the command deletes the BGP instance from the router.

Parameter	Description
<i>AS-NUMBER</i>	Specifies a 4-byte AS number in the range 1-4294967295 in integer format or from 0.1-65535.65535 in dotted format.

Examples

Configuring the BGP instance with the AS number:



Deleting BGP configurations:

```
switch(config)# no router bgp 100
This will delete all BGP configurations on this device.
Continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

router bgp vrf

```
router bgp <AS-NUMBER> [vrf <VRF-NAME>]
[no] router bgp <AS-NUMBER> [vrf <VRF-NAME>]
```

Description

This command configures VRF for the BGP instance.

The **no** form of this command removes the configuration.

Parameter	Description
<i>AS-NUMBER</i>	Specifies a 4-byte AS number in the range 1-4294967295 in integer format or from 0.1-65535.65535 in dotted format.
<i><VRF-NAME></i>	String VRF name for the VRF.

Usage

- Use the command **vrf vrf-name** within the router BGP context.
- **address-family {ipv4 | ipv6}** nodes are only supported within the VRF context.
- **address-family {ipv4 | ipv6}** nodes are required to redistribute the OSPF static/connected IPv4 or IPv6 routes.

Examples

Configure the VRF for customer A, on the BGP instance 100:

```
switch(config)# router bgp 100
switch(config)# vrf cust_a
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show bgp vpn unicast

```
show bgp [vrf <VRF-NAME>][{ipv4 unicast | ipv6 unicast| ipv4 unicast| all unicast}] [vsx-peer]
```

Description

Shows the BGP-VPN per VRF routes with additional route information like RD and extended community route targets.

Displays the BGP neighbor information for the specified VRF.



By default the default_vrf BGP instance information is displayed if the VRF is not specified.

Parameter	Description
unicast	Selects the subaddress family identifier
all	Displays VPNv4 address family routes for all VRFs
vrf	Displays VPNv4 address-family routes for specified VRF
vpn-addr-family	Required: Literal Select the VPNv4 or VPNv6 address family
vrf-name	Required: Literal or string. Specify all or vrf-name .
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Required use of *vpn-addr-family*:

```
switch# show bgp <vpn-addr-family> unicast {all | [vrf <vrf-name> | A.B.C.D/M]}
```

Show BGP VRF ipv4 unicast routes for vrf-name

```

switch# show bgp vrf Red ipv4 unicast
    Status codes: s suppressed, d damped, h history, * valid, > best, = multipath
    i internal, e external, S Stale, R Removed
    Origin codes: i - IGP, e - EGP, ? - incomplete

VRF: Red
Local Router-ID 172.16.3.1

Network          Nexthop      Metric  LocPrf  Weight Path
Route Distinguisher: 65000:1
*> 172.16.0.0/24  0.0.0.0        0       100     32768    ?
*> 172.16.1.0/24  0.0.0.0        0       100     32768    ?
*> 172.16.2.0/24  172.16.0.2     0       100     32768    ?
*> 172.16.3.0/24  172.16.0.3     0       100     32768    ?

Total number of entries 4

```

```

switch# show bgp vrf Green ipv4 unicast
    Status codes: s suppressed, d damped, h history, * valid, > best, = multipath
    i internal, e external, S Stale, R Removed
    Origin codes: i - IGP, e - EGP, ? - incomplete

VRF: Green
Local Router-ID 172.17.2.1

Network          Nexthop      Metric  LocPrf  Weight Path
Route Distinguisher: 65000:2
*> 172.17.0.0/24  0.0.0.0        0       100     32768    ?
*> 172.17.1.0/30  0.0.0.0        0       100     32768    ?
*> 172.17.2.0/24  172.17.0.2     0       100     32768    ?

Total number of entries 3

```

```

switch# show bgp vrf Blue ipv4 unicast
    Status codes: s suppressed, d damped, h history, * valid, > best, = multipath
    i internal, e external, S Stale, R Removed
    Origin codes: i - IGP, e - EGP, ? - incomplete

VRF: Blue
Local Router-ID 172.18.3.1

Network          Nexthop      Metric  LocPrf  Weight Path
Route Distinguisher: 65000:3
*> 172.18.0.0/24  0.0.0.0        0       100     32768    ?
*> 172.18.1.0/30  0.0.0.0        0       100     32768    ?
*> 172.18.3.0/24  172.18.0.3     0       100     32768    ?

Total number of entries 3

```

```

switch# show bgp vrf Shared ipv4 unicast
    Status codes: s suppressed, d damped, h history, * valid, > best, = multipath
    i internal, e external, S Stale, R Removed
    Origin codes: i - IGP, e - EGP, ? - incomplete

VRF: Shared

```

```

Local Router-ID 192.168.99.1

      Network          Nexthop      Metric  LocPrf  Weight Path
Route Distinguisher: 65000:99
*> 192.168.99.0/24  0.0.0.0      0        100    32768      ?

Total number of entries 1

```

Show BGP VRF ipv6 unicast routes for vrf-name:

```

switch# show bgp vrf Red ipv6 unicast
      Status codes: s suppressed, d damped, h history, * valid, > best, = multipath
      i internal, e external, S Stale, R Removed
      Origin codes: i - IGP, e - EGP, ? - incomplete

VRF: Red
Local Router-ID 172.16.3.1

      Network          Nexthop      Metric  LocPrf  Weight Path
Route Distinguisher: 65000:1
*   2001:100:1:1000:/56
      2001:100:1:1000::72a      0        0        200      ?
*> 2001:100:1:1000::/56
      ::                        0        100    32768      ?
*   2001:100:1:2000::/56
      ::FFFF:200.10.10.1 0      0        100    32768      ?

Total number of entries 3

```

Show BGP VRF routes for all vrfs and all address-families:

```

switch# show bgp all-vrf all
      Status codes: s suppressed, d damped, h history, * valid, > best, = multipath
      i internal, e external, S Stale, R Removed
      Origin codes: i - IGP, e - EGP, ? - incomplete

VRF: Blue
Local Router-ID 172.18.3.1

Address-family: IPv4 Unicast
-----
      Network          Nexthop      Metric  LocPrf  Weight Path
*> 172.18.0.0/24  0.0.0.0      0        100    32768      ?
*> 172.18.1.0/30  0.0.0.0      0        100    32768      ?
*> 172.18.3.0/24  172.18.0.3    0        100    32768      ?

Total number of entries 3

Address-family: IPv6 Unicast
-----
      Network          Nexthop      Metric  LocPrf  Weight Path

Toatl number of entries 0

VRF: Green
Local Router-ID 172.17.2.1

```



```

Address-family: IPv4 Unicast
-----
Network          Nexthop          Metric  LocPrf  Weight  Path
*> 172.17.0.0/24  0.0.0.0           0       100     32768   ?
*> 172.17.1.0/30  0.0.0.0           0       100     32768   ?
*> 172.17.2.0/24  172.17.0.2        0       100     32768   ?

Total number of entries 3

Address-family: IPv6 Unicast
-----
Network          Nexthop          Metric  LocPrf  Weight  Path

Total number of entries 0

VRF: Red
Local Router-ID 172.16.3.1

Address-family: IPv4 Unicast
-----
Network          Nexthop          Metric  LocPrf  Weight  Path
*> 172.16.0.0/24  0.0.0.0           0       100     32768   ?
*> 172.16.1.0/24  0.0.0.0           0       100     32768   ?
*> 172.16.2.0/24  172.16.0.2        0       100     32768   ?
*> 172.16.3.0/24  172.16.0.3        0       100     32768   ?

Total number of entries 4

Address-family: IPv6 Unicast
-----
Network          Nexthop          Metric  LocPrf  Weight  Path
* 2001:100:1:1000::/56
    2001:100:1:1000::72a    0       0       200     ?
*> 2001:100:1:1000::/56
    ::                    0       100     32768   ?
* 2001:100:1:2000::/56
    ::FFFF:200.10.10.1 0    0       100     32768   ?

Total number of entries 3

VRF: Shared
Local Router-ID 192.168.99.1

Address-family: IPv4 Unicast
-----
Network          Nexthop          Metric  LocPrf  Weight  Path
*> 192.168.99.0/24 0.0.0.0           0       100     32768   ?

Total number of entries 1

Address-family: IPv6 Unicast
-----
Network          Nexthop          Metric  LocPrf  Weight  Path

Total number of entries 0

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show bgp info vrf

```
show bgp info vrf <vrf-name> [vsx-peer]
```

Description

Displays BGP route-targets information for specified VRF.

Parameter	Description
info	Display BGP RT information.
vrf-name	Required string VRF name for the vrf.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Show BGP VRF information.

```
switch# show bgp info vrf red
VRF : red
VRF RD : 100:1

Address-family IPv4 unicast info
Redistribution : ospf
Export RT list : 100:1 100:2
Import RT list : 100:3

Address-family IPv6 unicast info
Redistribution : connected
Export RT list : 100:11 100:12
Import RT list : 100:15
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip route vrf

```
show ip route vrf <vrf-name> [vsx-peer]
```

Description

Shows route information for specified VRF.

Parameter	Description
<i>vrf-name</i>	Required: string VRF name for the VRF.
<i>vsx-peer</i>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show ip route vrf green

Displaying ipv4 routes selected for forwarding
'[x/y]' denotes [distance/metric]
  10.0.0.0/24, vrf green
    via 20.0.0.1[vrf red], [1/0], static
  30.0.0.0/24, vrf green
    via 1/1/2, [0/0], connected
30.0.0.2/32, vrf green
    via 1/1/2, [0/0], local
  60.0.0.0/24, vrf green
    via 1/1/1[vrf red], [1/0], static
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 route vrf

show ipv6 route vrf <VRF-NAME> [vsx-peer]

Description

Shows the route information for specified VRF.

Parameter	Description
<VRF-NAME>	Required: String VRF name for the VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying ipv4 routes selected for forwarding

```
switch(config)# show ip route vrf green
Origin Codes: C - connected, S - static, L - local
R - RIP, B - BGP, O - OSPF, D - DHCP
U - Unnumbered
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
IA - OSPF internal area, El - OSPF external type 1
E2 - OSPF external type 2
VRF: green
Prefix      Nexthop      Interface      VRF(egress)      Origin/
Distance/   Age
Type        Metric
-----
20.1.1.0/24      30.1.1.1      1/1/2          red               S
[1/0]          00h:00m:04s
30.1.1.0/24      -              1/1/2          red               B/I
[200/0]        00h:01m:05s
40.1.1.0/24      -              1/1/3          -                 C
[0/0]          -
40.1.1.1/32      -              1/1/3          -                 L
[0/0]          -
Total Route Count : 4
switch(config)#
switch(config)# show ip route vrf red
Displaying ipv4 routes selected for forwarding
Origin Codes: C - connected, S - static, L - local
R - RIP, B - BGP, O - OSPF, D - DHCP
U - Unnumbered
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
```

```

IA - OSPF internal area, E1 - OSPF external type 1
E2 - OSPF external type 2
VRF: red
Prefix          Nexthop    Interface    VRF(egress)    Origin/
Distance/      Age
Type          Metric
-----
30.1.1.0/24    -          1/1/2        -                C          [0/0]
-
30.1.1.1/32    -          1/1/2        -                L          [0/0]
-
40.1.1.0/24    -          1/1/3        green            B/I        [200/0]
00h:02m:42s
Total Route Count : 3

```

Displaying ipv6 routes selected for forwarding

```

Switch# show ipv6 route all-vrfs
Origin Codes: C - connected, S - static, L - local
R - RIP, B - BGP, O - OSPF, D - DHCP
U - Unnumbered
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
IA - OSPF internal area, E1 - OSPF external type 1
E2 - OSPF external type 2
VRF: green
Prefix          Nexthop    Interface    VRF(egress)    Origin/
Distance/      Age
Type          Metric
-----
2000::/64      3000::1    1/1/2        red            S
[1/0]          00h:01m:05s
3000::/64      -          1/1/2        red            B/I
[200/0]        00h:00m:16s
4000::/64      -          1/1/3        -              C
[0/0]          -
4000::1/128    -          1/1/3        -              L
[0/0]          -
VRF: red
Prefix          Nexthop    Interface    VRF(egress)    Origin/
Distance/      Age
Type          Metric
-----
3000::/64      -          1/1/2        -              C
[0/0]          -
3000::1/128    -          1/1/2        -              L
[0/0]          -
4000::/64      -          1/1/3        green          B/I
[200/0]        00h:00m:11s
Total Route Count : 7

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

vrf

```
vrf <VRF-NAME>
no vrf <VRF-NAME>
```

Description

Creates a VRF instance named <VRF-NAME> and then enters its context. Use **default** for <VRF-NAME> to enter the default VRF configure context.

Except for the default VRF, the **no** form of the command deletes the named VRF instance and any IP configuration for interfaces or SVI linked to default VRF. The default VRF cannot be deleted and a warning is given if attempted. To erase the Route-Distinguisher and Route-Targets, enter the default VRF context and delete them manually one by one.

Parameter	Description
<VRF-NAME>	Specifies the VRF name. Range: Up to 32 alphanumeric characters. The mgmt VRF cannot be used.

Examples

Creating the VRF named **cust_A** and then entering its context:

```
switch(config)# vrf cust_A
```

Entering the **default** VRF context:

```
switch(config)# vrf default
```

Deleting the VRF named **test**:

```
switch(config)# no vrf test
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Added default VRF information.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config</code>	Administrators or local user group members with execution rights for this command.

job

In the config context:

```
job <JOB-NAME>
no job [<JOB-NAME>]
```

Subcommands available In the job config context (config-job):

```
[no] enable
[no] desc <DESCRIPTION>
[no] [<SEQ-NUM>] [delay <DELAY>] cli <COMMAND>
resequence <START-SEQ-NUM> <INCREMENT>
```

Description

If **<JOB-NAME>** does not exist, this command creates a job and then enters its context.

The no form of this command deletes the specified job. If no job is specified, all jobs are deleted.



Deleting a job also removes it from any schedule that uses the job, preventing further attempts to execute the job.

If **<JOB-NAME>** exists, this command enters the **config-job-<NAME>** context for the specified job.

Parameter	Description
<JOB-NAME>	Specifies the job name. Range 1 to 64 characters (alphanumeric and "_" (underscore))

Subcommands

These subcommands are available within the **config-job-<NAME>** context for configuring the job:

enable

Enables the job (the default). **no enable** disables the job.

[no] desc <DESCRIPTION>

Specifies a user-defined job description. **no desc** removes the description. Range: 1 to 128 characters. For example:

```
switch(config-job-PTogl) # desc Toggle port 1/1/1
```

[no] [<SEQ-NUM>] [delay <DELAY>] cli <COMMAND>

Adds a CLI command to the job. The no form removes the command from the job. When executed, commands with simple (y/n) prompts (such as **boot system**) will be automatically confirmed with "y." Other commands requiring more complex user input (such as password change) cannot be used.

<SEQ-NUM> specifies the job CLI command sequence number to facilitate ordering of commands within a job. When omitted, a sequence number that is 10 greater the highest existing sequence

number is auto-assigned. The first auto-assigned sequence number is 10. Range: 1 to 4294967295.

[delay <DELAY>] specifies the delay in seconds before this CLI command is executed. The cumulative delay for all commands in a job must be no more than 300 seconds. Range 1 to 300.

cli <COMMAND> specifies the CLI command to be executed. Range 1 to 4096 characters.

These commands must not be used in a job: **copy, repeat, show boot-history, show core-dump, show events, show job, show tech, sleep, terminal-monitor.**

For example, adding a command as line 18 to a job:

```
switch(config-job-PTog1) # 18 cli interface 1/1/1
```

resequence <START-SEQ-NUM> <INCREMENT>

Resequences the CLI command line sequence numbers. Both **<START-SEQ-NUM>** and **<INCREMENT>** default to 10. For example, resequencing the CLI command list to start at 10 with an increment of 5.

```
switch(config-job-PTog1) # resequence 10 5
switch(config-job-PTog1) # show job PTog1
```

```
Job Name : PTog1
...
  Job CLI commands
  -----
    10 cli config
    15 cli interface 1/1/1
    20 cli shutdown
  ...
```

Usage

- A maximum of 20 commands can be used in a job.
- To see the maximum number of jobs and job execution output preserved instances for your particular switch, use command **show capacities job**.
- Jobs must complete execution in under five minutes and are force-stopped after five minutes if they do not.

Examples

Creating a port toggle job named **PTog1**:

```
switch(config) # job PTog1
switch(config-job-PTog1) # desc Toggle port 1/1/1
switch(config-job-PTog1) # 10 cli config
switch(config-job-PTog1) # 20 cli interface 1/1/1
switch(config-job-PTog1) # 30 cli shutdown
switch(config-job-PTog1) # 40 delay 10 cli no shutdown
switch(config-job-PTog1) # 50 cli end
switch(config-job-PTog1) # exit
switch(config) #
```

Creating a job named **Reboot_sw1** that saves the running configuration and then reboots the switch:

```

switch(config)# job Reboot_Sw1
switch(config-job-Reboot_Sw1)# desc Save config then reboot switch
switch(config-job-Reboot_Sw1)# 10 cli config
switch(config-job-Reboot_Sw1)# 20 cli write mem
switch(config-job-Reboot_Sw1)# 30 cli boot system
switch(config-job-Reboot_Sw1)# exit
switch(config)#

```



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config config-job- <i><NAME></i>	Administrators or local user group members with execution rights for this command.

reload

```

reload
  at YYYY-MM-DD HH:MM:SS
  after DD:HH:MM
  cancel

```

Description

Reboot the switch, stack, or chassis at a specific date and time up to 99 days in the future, or after a specified time period has elapsed. Reload information is not persistent after the reboot. The **reload** commands trigger a reload of the default image, which is defined using the **boot set-default** command. The **reload cancel** command cancels a scheduled reload operation.



The **reload** command cannot be issued if an In-Service Software Update (ISSU) is in progress.

Parameter	Description
at YYYY-MM-DD HH:MM:SS	On 4100i, 5420, 6000, 6100, 6300M/F, 6300L, 6400, 8100, 8320, 8325/8325H/8325P, 8360, 9300/9300S and 10000 switch series, specify the timestamp for the scheduled reload, where - YYYY represents the year. - MM represents the month, from 01 (January) to 12 (December). - DD represents the day (01 to 31). - HH represents the hour, in 24-hour clock format, 00-23. - MM represents the minute, 00-59.

Parameter	Description
	SS represents the seconds, 00-59.
after DD:HH:MM	On 4100i, 5420, 6000, 6100, 6300, 6400, 8100, 8320, 8325/8325H/8325P, 8360, 9300/9300S and 10000 switch series, specify how much time should elapse before the scheduled management module reload, where: - DD represents the number of days before the reload - HH represents the number of hours before the reload - MM represents the number of minutes before the reload.
cancel	Cancel any scheduled reload operations.

Usage

Configuring the reload feature will use one job scheduler space and reduce the number of available job scheduler configurations.

Examples

Scheduling a system reload on 4100i, 5420, 6000, 6100, 6300, 6400, 8100, 8320, 8325/8325H/8325P, 8360, 9300/9300S or 10000 switch series at a specific date and time:

```
switch# reload at 2025-08-12 12:01:00
Reload scheduled at 12:01:00 08/12/2025 (in 10 days, 15 hours, 17 minutes, 12
seconds)
The system will be rebooted at the scheduled time from the secondary image.
Continue (y/n)? y
Warning! Any change in configuration may be lost during the scheduled reboot.
Please remember to save the changes before the scheduled reboot happens.
Configuring reload feature will reduce one job configuration.
```

Scheduling a system reload on 4100i, 5420, 6000, 6100, 6300, 6400, 8100, 8320, 8325/8325H/8325P, 8360, 9300/9300S or 10000 switch series in one day and one hour from the current time:

```
switch# reload after 01:01:00
Reload scheduled in 1 days, 1 hours, 0 minutes
The system will be rebooted at the scheduled time from the secondary image.
Continue (y/n)? y
Warning! Any change in configuration may be lost during the scheduled reboot.
Please remember to save the changes before the scheduled reboot happens.
Configuring reload feature will reduce one job configuration.
```



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config config-job- <i><NAME></i>	Administrators or local user group members with execution rights for this command.

schedule

In the config context:

```
schedule <SCHEDULE-NAME> [transient]
no schedule [<SCHEDULE-NAME>]
```

Subcommands available In the schedule config context (config-schedule):

```
[no] enable
[no] desc <DESCRIPTION>
[no] [<SEQ-NUM>] job <JOB-NAME>
resequence <START-SEQ-NUM> <INCREMENT>
[no] trigger on HH:MM {daily | weekly <1-7> | monthly <1-31>}
    [count <1-1000>] [start YYYY-MM-DD]
[no] trigger every {days <1-365> | hours <1-8760> | minutes <30-525600>}
    [count <1-1000> ] [start HH:MM [YYYY-MM-DD]]
[no] trigger at HH:MM [YYYY-MM-DD]
```

Description

If **<SCHEDULE-NAME>** does not exist, this command creates a job schedule and then enters its context. The **no** form of this command deletes the specified schedule. If no schedule is specified, all schedules are deleted.

If **<SCHEDULE-NAME>** exists, this command enters the **config-schedule-*<NAME>*** context for the specified job schedule.

Parameter	Description
<i><SCHEDULE-NAME></i>	Specifies the schedule name. Range 1 to 64 characters (alphanumeric and "_" (underscore)).
[transient]	Causes the schedule to be cleared upon switch reboot. By default, schedules are maintained after switch reboots.

Subcommands

These subcommands are available within the **config-schedule-*<NAME>*** context for scheduling jobs and controlling the order in which the jobs are executed:

enable

Enables the schedule (the default). **no enable** disables the schedule.

[no] desc <DESCRIPTION>

Specifies a user-defined schedule description. **no desc** removes the description. Range: 1 to 128 characters. For example:

```
switch(config-schedule-Monthly)# desc Monthly schedule
```

[no] [<SEQ-NUM>] job <JOB-NAME>

Associates an existing job with this schedule. The **no** form removes the job from the schedule.

<JOB-NAME> specifies an existing job name. Range: 1 to 64 characters (alphanumeric and "_" (underscore)).

<SEQ-NUM> specifies the job name sequence number to facilitate ordering of jobs within a schedule. When omitted, a sequence number that is 10 greater than the highest existing sequence number is auto-assigned. The first auto-assigned sequence number is 10.

For example, associating two jobs with the selected schedule:

```
switch(config-schedule-Monthly)# 10 job PTog1
switch(config-schedule-Monthly)# 20 job PTog2
```

resequence <START-SEQ-NUM> <INCREMENT>

Resequences the job name sequence numbers in the schedule. Both **<START-SEQ-NUM>** and **<INCREMENT>** default to 10. For example, resequencing the job list to start at 5 with an increment of 10.

```
switch(config-schedule-Monthly)# resequence 5 10
switch(config-schedule-Monthly)# show schedule Monthly

Schedule Name: Monthly
...
  Scheduled Jobs
  -----
  5    : PTog1
  15   : PTog2
```

[no] trigger on HH:MM {daily | weekly <1-7> | monthly <1-31>}
[count <1-1000>] [start YYYY-MM-DD]

Sets the job to trigger at a specific time. The **no** form removes the trigger.

HH:MM selects the time using a 24-hour clock (switch local time). Range: 00:00 to 23:59.

daily selects daily.

weekly <1-7> selects specific days of week or days-of-week ranges (with comma or hyphen separators) using numeric day-of-week numbers with Sunday equal 1. For example: 1, 3, 5-7 for Sunday, Tuesday, Thursday, Friday, Saturday.

monthly <1-31> selects specific days of month or days of month ranges (with comma or hyphen separators) using numeric day-of-month numbers. For example: 5, 14-21, 25, 31. For months with fewer days than the specified day number, the last day of the month is selected.

count <1-1000> selects the number of times the job will be executed. When omitted, job execution triggering is indefinite.

start YYYY-MM-DD selects the schedule first trigger date. When omitted, today's date is used for times at least 5 minutes into the future, otherwise tomorrow is selected as the first trigger date.

For example, setting the schedule to trigger monthly on the 15th, at 11:45 PM, starting on August 15, with an execution limit of 200:

```
switch(config-schedule-M)# trigger on 23:45 monthly 15 count 200 start 2021-08-15
```

[no] trigger every {days <1-365> | hours <1-8760> | minutes <30-525600>}
[count <1-1000>] [start HH:MM [YYYY-MM-DD]]

Sets the job trigger to a specific periodic interval. The **no** form removes the trigger. By default, the schedule is activated within 5 minutes from the configuration time. If the start time is specified, then the job is executed beginning at the specified start time and thereafter at the specified interval.

days <1-365> selects the interval in days. Range: 1 to 365.

hours <1-8760> selects the interval in minutes. Range: 1 to 8760.

minutes <30-525600> selects the interval in seconds. Range: 30 to 525600.

count <1-1000> selects the number of times the job will be executed. When omitted, job execution triggering is indefinite.

start HH:MM [YYYY-MM-DD] selects the schedule first trigger time and date.

For example, setting the schedule to trigger once every 14 days, starting on January 1, with an execution limit of 500:

```
switch(config-schedule-Ev14D)# trigger every days 14 count 500 start 2022-01-01
```

[no] **trigger** at HH:MM [YYYY-MM-DD]

Sets the job to trigger one time only on a specific date and time. When the date is omitted, today's date is used for times at least 5 minutes into the future, otherwise tomorrow is selected. The no form removes the trigger.

For example, setting the schedule to trigger once only on August 26 at midnight:

```
switch(config-schedule-Aug26)# trigger at 00:00 2021-08-26
```

Usage

- A job can be used only once per schedule.
- To see the maximum number of schedules and jobs per schedule for your particular switch, use command **show capacities schedule**.
- Configure the jobs to be executed (using the **job** command) before configuring a schedule.
- Jobs must complete execution in under five minutes and are force-stopped after five minutes if they do not.
- A job must be scheduled to execute at least five minutes after its previous execution. If the same job is scheduled to be executed again within less than five minutes, the execution is skipped.

Examples

Creating a schedule named **PT2xW** that runs the port toggle job **PTog1** on Mondays and Fridays at 11:45 PM, starting on August 2 2021, with a one-year duration:

```
switch(config)# schedule PT2xW
switch(config-schedule-PT2xW)# desc Monday & Friday 11:45 PM port toggles
switch(config-schedule-PT2xW)# 10 job PTog1
switch(config-schedule-PT2xW)# trigger on 23:45 weekly 2,6 count 104 start 2021-08-02
switch(config-schedule-PT2xW)# exit
switch(config)#
```

Creating a schedule named **RB_LDM** that runs the switch reboot job on the last day of the month at 3:00 AM, starting on January 31 2022, with a two-year duration:

```
switch(config)# schedule RB_LDM
switch(config-schedule-RB_LDM)# desc Monthly reboot 3:00 AM
switch(config-schedule-RB_LDM)# 10 job Reboot_sw1
switch(config-schedule-RB_LDM)# trigger on 3:00 monthly 31 count 24 start 2022-01-31
```

```
switch(config-schedule-RB_LDM) # exit
```



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config config-schedule- <i><NAME></i>	Administrators or local user group members with execution rights for this command.

show job

```
show job [<JOB-NAME>] [execution-output <INSTANCE-ID>]
```

Description

Shows information about a specific job or every job. Optionally shows the job execution output log.

Parameter	Description
<i><JOB-NAME></i>	Specifies an existing job name. When omitted, information is shown for every job. Range: 1 to 64 characters (alphanumeric and "_" (underscore)).
<i><INSTANCE-ID></i>	Selects the job execution output instance with 1 selecting the most recent. To see the maximum number of job execution output instances for your particular switch, use command show capacities job .

Usage

Job execution statistics such as execution counts are reset to zero upon switch reboot.

Examples

Showing port toggle job information before execution has occurred:

```
switch# show job PTog1

Job Name : PTog1

Enabled           : Yes
Description       : Toggle port 1/1/1
```

```
Status                : waiting
Number of commands    : 5
Total execution count  : 0
Failed execution count : 0
```

Job CLI commands

```
10 cli config
20 cli interface 1/1/1
30 cli shutdown
40 delay 10 cli no shutdown
50 cli end
```

Showing port toggle job information after execution has occurred:

```
switch# show job PTog1
```

Job Name : PTog1

```
Enabled                : Yes
Description             : Toggle port 1/1/1
Status                 : waiting
Number of commands     : 5
Total execution count   : 1
Failed execution count  : 0
```

Job execution history

```
Instance number        : 1
Execution status        : success
Execution start time    : Mon Aug 2 23:45:00 2021
Execution duration      : 10s
```

Job CLI commands

```
10 cli config
20 cli interface 1/1/1
30 cli shutdown
40 delay 10 cli no shutdown
50 cli end
```

Showing port toggle job most recent execution output:

```
switch# show job PTog1 execution-output 1
```

=====

Command: config

time: Mon Aug 2 23:45:00 2021

=====

=====

Command: interface 1/1/1

time: Mon Aug 2 23:45:00 2021

=====

=====

Command: shutdown

time: Mon Aug 2 23:45:00 2021


```

=====

Command: cli no shutdown
time: Mon Aug  2 23:45:10 2021
=====

Command: end
time: Mon Aug  2 23:45:10 2021
=====

```



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show capacities (job, schedule)

`show capacities {job | schedule}`

Description

Shows either job or schedule capacities information for your switch model.

Examples

Showing job capacities information (8320 example shown):

```

switch# show capacities job

System Capacities: Filter Job
Capacities Name                                     Value
-----
Maximum number of job execution output preserved per job      10
Maximum number of jobs configurable in a system                32

```

Showing schedule capacities information (8320 example shown):

```
switch# show capacities Schedule
```

```
System Capacities: Filter Schedule
```

Capacities Name	Value
Maximum number of jobs configurable in a schedule	10
Maximum number of schedules configurable in a system	32



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show reload

```
show reload
```

Description

Display the configuration defined using the [reload](#) command.

Examples

Displaying the reload configuration on a 4100i, 5420, 6000, 6100, 6300, 6400, 8100, 8320, 8325/8325H/8325P, 8360, 9300/9300S or 10000 switch series:

```
switch# show reload
-----
Reload Configuration
-----
Module           : Chassis
Reboot after     : 2 days, 8 hours, 10 minutes
-----
```



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config config-job- <i><NAME></i>	Administrators or local user group members with execution rights for this command.

show running-config (job, schedule)

show running-config [current-context]

Description

Shows the entire running configuration for the switch, including configuration details for the Job Scheduler job and schedule configuration.

Parameter	Description
current-context	When included from within the Job Scheduler job or schedule context, shows only the job or schedule configuration information for the selected job or schedule.

Examples

Showing the running configuration information for all jobs and schedules with unrelated configuration information omitted for clarity (omitted portions represented by ellipses("...")):

```
switch# show running-config

Current configuration:
...
!
job PTog1
  desc Toggle port 1/1/1
  10 cli config
  20 cli interface 1/1/1
  30 cli shutdown
  40 delay 10 cli no shutdown
  50 cli end
job Reboot_sw1
  desc Save config then reboot switch
  10 cli config
  20 cli write mem
  30 cli boot system
schedule PT2xW
  desc Monday & Friday 11:45 PM port toggles
  trigger on 23:45 weekly 2,6 count 104 start 2021-08-02
  10 job PTog1
schedule RB_LDM
  desc Monthly reboot 3:00 AM
  trigger on 3:00 monthly 31 count 24 start 2022-01-31
  10 job Reboot_sw1
```

...

From within the job **PTog1** context, showing the running configuration information for the job:

```
switch(config-job-PTog1)# show running-config current-context

Current configuration:
job PTog1
  desc Toggle port 1/1/1
  10 cli config
  20 cli interface 1/1/1
  30 cli shutdown
  40 delay 10 cli no shutdown
  50 cli end
```

From within the schedule **PT2xW** context, showing the running configuration information for the schedule:

```
switch(config-schedule-PT2xW)# show running-config current-context

Current configuration:
schedule PT2xW
  desc Monday & Friday 11:45 PM port toggles
  trigger on 23:45 weekly 2,6 count 104 start 2021-08-02
  10 job PTog1
```



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#) config-job- <i><NAME></i> config-schedule- <i><NAME></i>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show schedule

```
show schedule [<SCHEDULE-NAME>]
```

Description

Shows information about a specific schedule or every schedule.

Parameter	Description
<SCHEDULE-NAME>	Specifies an existing job schedule name. When omitted, information is shown for every schedule. Range: 1 to 64 characters (alphanumeric and "_" (underscore)).

Usage

Schedule statistics such as **Triggered count** are reset to zero upon switch reboot.

Examples

Showing port toggle job schedule information before execution has occurred:

```
switch# show schedule PT2xW

Schedule Name: PT2xW

Schedule config
-----
Description      : Monday & Friday 11:45 PM port toggles
Enabled          : Yes
Trigger type     : calendar
Transient        : No
Max trigger count : 104
Trigger start date : 2021-08-02 23:45

Schedule Status
-----
Trigger status   : active
Next trigger time : Mon Aug  2 23:45:00 2021

Scheduled Jobs
-----
10  : PTogl
```

Showing port toggle job schedule information after execution has occurred:

```
switch# show schedule PT2xW

Schedule Name: PT2xW

Schedule config
-----
Description      : Monday & Friday 11:45 PM port toggles
Enabled          : Yes
Trigger type     : calendar
Transient        : No
Max trigger count : 104
Trigger start date : 2021-08-02 23:45

Schedule Status
-----
Trigger status   : active
Next trigger time : Fri Aug  6 23:45:00 2021
Triggered count  : 1

Scheduled Jobs
```

10 : PTog1



For more information on features that use this command, refer to the Job Scheduler Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

accept-lifetime

```
accept-lifetime [start-time <time> <month>/<day>/<year>] {duration {<seconds> | infinite}  
| end-time <time> <month>/<day>/<year>}
```

Description

Configures the duration for which the key is valid for receiving packets.

The **no** form of this command configures the key packet receiving duration to the default value of an infinite time.

Parameter	Description
start-time	Time at which the key chain lifetime starts. Required. Format: HH:MM:SS
end-time	Time at which the key chain lifetime expires. Required. Format: HH:MM:SS
day	Day of the month. Required. Range: 1-31.
month	Month of the year. Required.
year	Year. Required. Range: 2020-2050
duration	Time in seconds. Optional. Range: 1-2147483646.
infinite	Specifies infinite time for the key. Optional.

Examples

Configuring the duration for which the key is valid for receiving packets:

```
switch# configure terminal  
switch(config)# keychain ospf_keys  
switch(config-keychain)# key 1  
switch(config-keychain-key)# accept-lifetime start-time 10:10:10 10/25/2020 end-  
time 10:10:10 11/25/2020  
switch(config-keychain-key)# accept-lifetime start-time 10:10:10 10/25/2020  
duration 1000  
switch(config-keychain-key)# accept-lifetime start-time 10:10:10 10/25/2020  
duration infinite  
switch(config-keychain-key)# accept-lifetime end-time 10:10:10 11/25/2020  
switch(config-keychain-key)# accept-lifetime duration 1000  
switch(config-keychain-key)# accept-lifetime duration infinite
```

Configuring the key packet receiving duration to the default value of an infinite time:

```
switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# no accept-lifetime
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-keychain-key	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

cryptographic-algorithm

```
recv-id cryptographic-algorithm {aes-cmac-128 | hmac-sha-1 | hmac-sha-256 | hmac-sha-384 |
hmac-sha-512 | md5}
no cryptographic-algorithm
```

Description

Configures the recv-id cryptographic algorithm for the key. The key will not be valid until the [receive ID](#), the [send ID](#), and [send lifetime](#) is configured for [TCP-AO](#). Choose one of the authentication algorithms from the following parameters. The **no** form of this command configures the default cryptographic algorithm for a key, md5.



TCP Authentication Option (TCP-AO) authentication supports only the *aes-cmac-128* and *hmac-sha-1* algorithms. If you are configuring TCP-AO, you must select one of these options.

Parameter	Description
aes-cmac-128	Sets the authentication algorithm for the key to AES-CMAC-128. This parameter is only supported for TCP-AO.
hmac-sha-1	Sets the authentication algorithm for the key to SHA-1. This parameter is also supported for TCP-AO.
hmac-sha-256	Sets the authentication algorithm for the key to SHA-256.
hmac-sha-384	Sets the authentication algorithm for the key to SHA-384.
hmac-sha-512	Sets the authentication algorithm for the key to SHA-512.

Parameter	Description
md5	Sets the authentication algorithm for the key to md5. Maximum length of the key string supported: 16 bytes (config-if context), 64 bytes (config-keychain-key context).

Examples

Set the authentication algorithm for the key to **SHA-384**:

```
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# recv-id cryptographic-algorithm hmac-sha-384
```

Set the authentication algorithm to the default, **md5**:

```
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# no recv-id cryptographic-algorithm
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.11	The aes-cmac-128 parameter is introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-keychain-key	Administrators or local user group members with execution rights for this command.

key

key <KEY-ID>

Description

Creates the key for a key chain and enters the key chain key context. A maximum of 64 keys can be configured per key chain.

The **no** form of this command deletes the key from the key chain.

Parameter	Description
<KEY-ID>	ID of the key. Required. Range: 1-255.

Examples

Creating a key for a key chain:

```
switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
```

Deleting a key from a key chain:

```
switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# no key 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-keychain	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

keychain

keychain <KEYCHAIN-NAME>

Description

Creates the key chain and enters the key chain context. A maximum of 64 key chains can be configured in the system.

The **no** form of this command removes the key chain if it is not used by any subscribers.

Parameter	Description
<KEYCHAIN-NAME>	Name of the key chain. Required.

Examples

Creating a key chain:

```
switch# configure terminal
switch(config)# keychain ospf_keys
```

Removing a key chain:

```
switch# configure terminal  
switch(config)# keychain ospf_keys
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

key-string

key-string [{ciphertext | plaintext} <PASSWORD>]

Description

Sets the key password. The password is internally stored in encrypted form. The key is not valid until its password has been set.

The **no** form of this command deletes the password used for the key.

Parameter	Description
ciphertext	Specifies that the key password is provided as ciphertext.
plaintext	Specifies that the key password is provided as plaintext.
<PASSWORD>	Specifies the key password.



When the key password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Setting the key password with plaintext:

```
switch(config)# keychain ospf_keys  
switch(config-keychain)# key 1  
switch(config-keychain-key)# key-string plaintext F82#450bHP
```

Setting the key password with plaintext prompting:

```
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# key-string
Enter the key password: *****
Re-Enter the key password: *****
```

Setting the key password with ciphertext:

```
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# key-string ciphertext AQBpfciFZ/P...biAAAOjc0a8=
```

Deleting the password for the key:

```
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# no key-string
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-keychain-key	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

name

name <KEY-NAME>
no name <KEY-NAME>

Description

Configures a name for a numbered key in a key chain.
The **no** form of this command removes the name of the key.

Parameter	Description
<KEY-NAME>	Specifies the name of the key in alphanumeric characters. Range: 1-64.

Examples

Creating a name for a key in a key chain called **abcdef123456**:

```
switch# configure terminal
switch(config)# keychain macsec_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# name abcdef123456
```

Removing the name of the key named **abcdef123456**:

```
switch# configure terminal
switch(config)# keychain macsec_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# no name abcdef123456
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.11	Command added.

Command Information

Platforms	Command context	Authority
All platforms	config-keychain-key	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

recv-id

recv-id <0-255>

Description

Configures the receive ID for a keychain key. The receive ID has to be unique across keys in the keychain.

The **no** form of this command configures removes the recv-id value. The receive ID can not be changed for an active key of a keychain which is associated with BGP neighbor.

Parameter	Description
<0-255>	Set the receive ID corresponding to the keychain key. Supported values are 0-255.

Examples

Configuring the receive ID for the keychain key.

```
switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# recv-id 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-keychain-key	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

send-lifetime

```
send-lifetime [start-time <time> <month>/<day>/<year>] {duration {<seconds> | infinite} |
end-time <time> <month>/<day>/<year>}
```

Description

Configures the duration for which the key is valid for sending packets.

The **no** form of this command configures the key packet sending duration to the default value of an infinite time.

Parameter	Description
start-time	Time at which the key chain lifetime starts. Required. Format: HH:MM:SS
end-time	Time at which the key chain lifetime expires. Required. Format: HH:MM:SS
day	Day of the month. Required. Range: 1-31.
month	Month of the year. Required.
year	Year. Required. Range: 2020-2050
duration	Time in seconds. Optional. Range: 1-2147483646.
infinite	Specifies infinite time for the key. Optional.

Examples

Configuring the duration for which the key is valid for sending packets:

```

switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2020 end-time
10:10:10 11/25/2020
switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2020 duration
1000
switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2020 duration
infinite
switch(config-keychain-key)# send-lifetime end-time 10:10:10 11/25/2020
switch(config-keychain-key)# send-lifetime duration 1000
switch(config-keychain-key)# send-lifetime duration infinite

```

Configuring the key packet sending duration to the default value of an infinite time:

```

switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# no send-lifetime

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-keychain-key	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

send-id

send-id <0-255>

Description

Configures the send ID for a keychain key. The send ID has to be unique across keys in the keychain. The **no** form of this command configures removes the send-id value. The send id can not be changed for an active key of a keychain which is associated with BGP neighbor.

Parameter	Description
<0-255>	Set the send ID corresponding to the keychain key. Supported values are 0-255.

Examples

Configuring the send ID for the keychain key.

```
switch# configure terminal
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# send-id 218
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-keychain-key	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show capacities keychain

show capacities keychain

Description

Shows the maximum number of key chains and keys configurable in a key chain.

Example

```
switch# show capacities keychain

System Capacities: Filter Keychain
Capacities Name      Value
-----
Maximum number of keychains supported in the system
64
Maximum number of Keys supported in a single Keychain
64
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>)	Administrators or local user group members with execution rights for this command.

show keychain

show keychain [<KEYCHAIN-NAME>]

Description

Shows information about configured and active keys of a named key chain or (if **keychain-name** is not specified) all configured key chains.

Parameter	Description
<KEYCHAIN-NAME>	Name of the key chain. Optional.

Example

```
switch# show keychain
Keychain Name : macsec_keys
  Number of Keys      : 1
  Active Send Key ID  :
  Active Recv Key IDs :

  Key ID : 1
    Key name      : abcdef123456
    Key string     :
  AQBapYa+0qQDzcakbB1TopeX0AMYDDWDW015orkH5mY3qJDaBAAAADASiBQ=
    Send Key Validity : 00:00:00 01/01/2020 to Infinite
    Recv Key Validity : 00:00:00 01/01/2020 to Infinite

Keychain Name : ospf_keys
  Number of Keys      : 2
  Active Send Key ID  : 7
  Active Recv Key IDs : 7, 200

  Key ID      : 7
    Key name   : -
    Key string :
  AQBapZlOHio9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
    Crypto-Algorithm : sha256
    Send Key Validity : 00:00:01 10/1/2020 to 23:59:01 10/1/2021
    Recv Key Validity : 00:00:01 10/1/2020 to infinite
  Key ID      : 200
    Key name   : -
    Key string :
  AQBapZlOHio9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
    Crypto-Algorithm : sha512
```

```

    Send Key Validity : 00:00:01 10/1/2020 to 23:59:01 10/1/2021
    Recv Key Validity : 00:00:01 10/1/2020 to 23:59:01 10/1/2021

Keychain Name : bgp_keys
  Number of Keys      : 2
  Active Send Key ID  : 7
  Active Recv Key IDs : 7

  Key ID      : 7
  Key name    : -
  Key string   :
  AQBapZl0HiO9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
  Crypto-Algorithm : md5
  Send Key Validity : 00:00:01 10/26/2020 to 23:59:01 10/1/2021
  Recv Key Validity : 00:00:01 10/22/2020 to infinite
  Key ID      : 8
  Key name    : -
  Key string   :
  AQBapZl0HiO9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
  Crypto-Algorithm : sha384
  Send Key Validity : 00:00:01 10/1/2021 to 23:59:01 10/1/2021
  Recv Key Validity : 00:00:01 10/1/2021 to 23:59:01 10/1/2021
  ...
  ...

Keychain Name : ospf_keys
  Number of Keys      : 2
  Active Send Key ID  : 7
  Active Recv Key IDs : 7, 200

  Key ID      : 7
  Key name    : -
  Key string   :
  AQBapZl0HiO9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
  Crypto-Algorithm : sha256
  Send Key Validity : 00:00:01 10/1/2020 to 23:59:01 10/1/2021
  Recv Key Validity : 00:00:01 10/1/2020 to infinite
  Key ID      : 200
  Key name    : -
  Key string   :
  AQBapZl0HiO9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
  Crypto-Algorithm : sha512
  Send Key Validity : 00:00:01 10/1/2020 to 23:59:01 10/1/2021
  Recv Key Validity : 00:00:01 10/1/2020 to 23:59:01 10/1/2021

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>)	Administrators or local user group members with execution rights for this command.

show running-config keychain

show running-config keychain

Description

Shows the configurations for key chain protocol.

Example

```
switch# show running-config keychain
keychain ospf_keys
  key 1
    key-string ciphertext
    AQBapZlOHio9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
    cryptographic-algorithm md5
    accept-lifetime start-time 10:10:10 10/25/2020 end-time 10:10:10 11/25/2020
    send-lifetime start-time 10:10:10 10/25/2020 end-time 10:10:10 11/25/2020
  key 45
    key-string ciphertext
    AQBapZlOHio9W3JwRqnjtLfbV73BPLS1S6TGVg+Lzl7N4e5eBAAAAPWaPBE=
    accept-lifetime start-time 10:10:10 10/25/2020 end-time 10:10:10 11/25/2020
  key 33
keychain macsec_keys
  key 1
    name abcdef123456
    key-string ciphertext
    AQBapYa+0qQDzcakbB1TopeX0AMYDDWDW015orkH5mY3qJDaBAAAADASiBQ=
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>)	Administrators or local user group members with execution rights for this command.

show interface

```
show interface [<IFNAME>|<IFRANGE>] [brief | physical]
show interface [<IFNAME>|<IFRANGE>] [extended [non-zero] | [human-readable]]
show interface [<IFNAME>] monitor [human-readable]
show interface [lag | loopback | tunnel | vlan ] [<ID>] [brief]
show interface lag [<LAG-ID>] [extended [non-zero] | [human-readable]]
show interface lag [<LAG-ID>] monitor [human-readable]
show interface vxlan <VXLAN-ID> [brief | physical]
show interface vxlan <VXLAN-ID> [brief | physical]
```

Description

Shows active configurations and operational status information for interfaces.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
brief	Shows brief info in tabular format.
physical	Shows the physical connection info in tabular format.
extended	Shows additional statistics, including the tx filtered and rx filtered counters. ▪ Rx filter packets are protocol packets received when the protocol is disabled on the switch and there is only one port in the VLAN. Protocols include OSPF, PIM, RIP, LACP, and LLDP. ▪ An example of a Tx filtered packet would be a multicast packet being filtered from going out of the ingress port.
human-readable	Shows statistics rounded to the nearest power of 1000, for example, 1K, 345M, 2G. This is available only in the CLI interface output.
non-zero	Shows only non zero statistics.
LAG	Shows LAG interface information.
monitor	Continuously monitor interface statistics.
LOOPBACK	Shows loopback interface information.
TUNNEL	Shows tunnel interface information.
VLAN	Shows VLAN interface information.
<LAG-ID>	Specifies the LAG number. Range: 1-256
<LOOPBACK-ID>	Specifies the LOOPBACK number. Range: 0-255
<TUNNEL-ID>	Specifies the tunnel ID. Range: 1-255
<VLAN-ID>	Specifies the VLAN ID. Range: 1-4094
VXLAN	Shows the VXLAN interface information.
<VXLAN-ID>	Specifies the VXLAN interface identifier. Default: 1

Examples

Showing interface information when it is configured as a route-only port:

```
switch# show interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Link state: up for 2 days (since Sun Jun 21 05:30:22 UTC 2020)
```

```

Link transitions: 1
Description: backup data center link
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 1500
Type 1GbT
Full-duplex
qos trust none
Speed 1000 Mb/s
Auto-negotiation is on
Flow-control: off
Error-control: off
L3 Counters: Rx Enabled, Tx Enabled
Rate collection interval: 300 seconds

```

Rates	RX	TX	Total (RX+TX)
Mbits / sec	0.00	0.00	0.00
KPkts / sec	0.00	0.00	0.00
Unicast	0.00	0.00	0.00
Multicast	0.00	0.00	0.00
Broadcast	0.00	0.00	0.00
Utilization %	0.00	0.00	0.00

Statistics	RX	TX	Total
Packets	0	0	0
Unicast	0	0	0
Multicast	0	0	0
Broadcast	0	0	0
Bytes	0	0	0
Jumbos	0	0	0
Dropped	0	0	0
Filtered	0	0	0
Pause Frames	0	0	0
L3 Packets	0	0	0
L3 Bytes	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0
Other	0	0	0

Showing information when the interface is currently linked at a downshifted speed:

```

switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...
Auto-negotiation is on with downshift active

```

Showing information when the interface is shut down during a VSX split:

```

switch(config-if)# show interface 1/1/1
Interface 1/1/1 is down
Admin state is up
State information: Disabled by VSX
Link state: down for 3 days (since Tue Mar 16 05:20:47 UTC 2021)
Link transitions: 0
Description:
Hardware: Ethernet, MAC Address: 04:09:73:62:90:e7

```

```

MTU 1500
Type SFP+DAC3
Full-duplex
qos trust none
Speed 0 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: 1502-1505
Rate collection interval: 300 seconds

```

Rate	RX	TX	Total (RX+TX)
Mbits / sec	0.00	0.00	0.00
KPkts / sec	0.00	0.00	0.00
Unicast	0.00	0.00	0.00
Multicast	0.00	0.00	0.00
Broadcast	0.00	0.00	0.00
Utilization	0.00	0.00	0.00

Statistic	RX	TX	Total
Packets	0	0	0
Unicast	0	0	0
Multicast	0	0	0
Broadcast	0	0	0
Bytes	0	0	0
Jumbos	0	0	0
Dropped	0	0	0
Pause Frames	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0

Showing the monitor information:



In monitor mode, the CLI refreshes data automatically until it is exited by entering **q**. Pressing **?** opens the help menu to display which options are available in this context.

Interface 1/1/1 is up			
Rate	RX	TX	Total (RX+TX)
MBits / sec	30196.43	30196.43	60392.85
MPkts / sec	58977.39	58977.40	117954.79
Unicast	0.00	0.00	0.00
Multicast	58977.39	58977.40	117954.79
Broadcast	0.00	0.00	0.00
Utilization %	75.49	75.49	150.98
Statistic	RX	TX	Total (RX+TX)
Packets	4756527649	4756527865	9513055514
Unicast	0	0	0
Multicast	4756527649	4756527865	9513055514
Broadcast	2	0	2
Bytes	304417778668	304417795428	608835574096

```

Jumbos                0                0                0
Dropped                0            19028847730        19028847730
Pause Frames           0                0                0
Errors                 0                0                0
CRC/FCS                0                n/a            0
help: ?, quit: q

```

```

Help for Interface Monitor
h  Toggle human-readable mode
c  Clear interface statistics
Does not apply to rates
Arrows, PgUp, PgDn, Home, End
Navigate interface statistics
Delay: 2
help: ?, quit: q

```

Showing the output for interface 1/1/1 in human-readable format:



In human-readable format, the **< 1** symbol for **Utilization** indicates that the amount of packets is between zero and one. This is true in cases where the number of bytes increases but the number of packets and the **Utilization** value is not displayed even in the normal output, where the human-readable parameter is not included in the command.

```

switch(config-if)# show interface 1/1/1 human-readable
Interface 1/1/1 is up

```

Rate	RX	TX	Total (RX+TX)
Bits / sec	3M	3M	6M
Pkts / sec	316	316	633
Unicast	319	319	638
Multicast	0	0	0
Broadcast	0	0	0
Utilization %	< 1	< 1	< 1

Statistic	RX	TX	Total
Packets	577K	577K	1M
Unicast	577K	577K	1M
Multicast	0	51	51
Broadcast	0	15	15
Bytes	744M	745M	1G
Jumbos	0	0	0
Dropped	0	0	0
Filtered	0	0	0
Pause Frames	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0

Showing information about extended counters:



The output of the `show interface extended` command varies depending on the switch model and configuration.

```
switch(config-if)# show interface 1/1/17 extended
```

```
-----
```

```
Interface 1/1/17
```

```
-----
```

Statistics	Value
Dot1d Tp Port In Frames	547
Dot1d Tp Port Out Frames	608
Dot3 In Pause Frames	0
Dot3 Out Pause Frames	0
Ethernet Stats Broadcast Packets	19
Ethernet Stats Bytes	40162
Ethernet Stats Packets	342
...	

```
-----
```

Error-Statistics	Value
Dot1d Base Port MTU Exceeded Discards	0
Dot3 Control In Unknown Opcodes	0
Dot3 Stats Alignment Errors	0
Dot3 Stats FCS Errors	0
Dot3 Stats Frame Too Longs	0
Dot3 Stats Internal Mac Transmit Errors	0
Ethernet RX Oversize Packets	0
...	

```
-----
```

Showing interface link-status:

```
switch# show interface link-status
```

```
-----
```

Port	Type	Physical Link State	Link Transitions	Last Change
1/1/1	1G-BT	down	0	--
1/1/2	1G-BT	up	1	1 minute ago (Fri Mar 09 12:36:56 UTC 2018)
1/1/3	1G-BT	up	1	1 minute ago (Fri Mar 09 12:36:56 UTC 2018)
1/1/4	--	down	0	--
1/1/5	--	down	0	--

Showing interface loopback 1 link-status:

```
-----
```

Port	Type	Physical Link State	Link Transitions	Last Change
loopback1	--	up	--	--

```
-----
```

Showing interface 1/1/2-1/1/3 link-status:

```
-----
```

Port	Type	Physical Link State	Link Transitions	Last Change

```
-----
```



```

1/1/2          1G-BT          up          1          1 minute ago (Fri Mar 09
12:36:56 UTC 2018)
1/1/3          1G-BT          up          1          1 minute ago (Fri Mar 09
12:36:56 UTC 2018)

```

Showing interface link-status:

```

switch# show interface link-status
-----
Port           Type           Physical      Link           Link Flaps      Last
Link State     Transitions    Ignored        Change
-----
1/1/1          1G-BT          down          0              0              --
1/1/2          1G-BT          up            1              0              1 minute ago
(Fri Mar 09 12:36:56 UTC 2018)
1/1/3          1G-BT          up            1              0              1 minute ago
(Fri Mar 09 12:36:56 UTC 2018)
1/1/4          --             down          0              0              --
1/1/5          --             down          0              0              --

```

Showing state information when interface is blocked:

```

8360(config-if)# show interface 1/1/1

Interface 1/1/1 is up (Blocked)
Admin state is up
State information: Blocked by UDLD
Link state: up for 1 minute (since Mon Jun 10 09:25:27 UTC 2024)
Link transitions: 1
Description:
Persona:
Hardware: Ethernet, MAC Address: 00:fd:45:67:85:91
MTU 1500
Type 10G-LR / 10G SFP+ LR
Full-duplex
qos trust none
Speed 10000 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: access
Access VLAN: 1
Rate collection interval: 300 seconds

Rate           RX           TX           Total (RX+TX)
-----
Mbits / sec    0.00          0.00          0.00
KPkts / sec    0.00          0.00          0.00
Unicast         0.00          0.00          0.00
Multicast       0.00          0.00          0.00
Broadcast       0.00          0.00          0.00
Utilization %   0.00          0.00          0.00
Statistic       RX           TX           Total
-----
Packets        15           15           30
Unicast         12           12           24
Multicast        3            3            6
Broadcast        0            0            0
Bytes          1350         1350         2700

```

Jumbos	0	0	0
Dropped	0	0	0
Pause Frames	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

Command History

Release	Modification
10.15	Added state information when port goes into down state.
10.11	Added <code>monitor</code> parameter.
10.10	Added <code>human-readable</code> parameter.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

description

description <TEXT>
no description <TEXT>

Description

Provides a brief description of the LAG interface. The description text is saved in the configuration of the LAG. It is available even after a reboot.

The no form of this command removes the description of the LAG interface from the configuration.

Parameter	Description
<TEXT>	Specifies the description of the LAG interface.

Example

```
switch(config)# interface lag 10
switch(config-lag-if)# description This LAG is used for an example.
switch(config-lag-if)# show running-config
...
vlan 1
interface lag 10
    description This LAG is used for an example.
interface lag 60
switch(config-lag-if)#
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-lag-if	Administrators or local user group members with execution rights for this command.

interface lag

```
interface lag <ID>  
no interface lag <ID>
```

Description

Creates a Link Aggregation Group (LAG) interface represented by an ID.

The **no** form of this command deletes a LAG interface represented by an ID.

Parameter	Description
<ID>	Specifies a LAG interface ID.

Usage

Keep in mind the following requirements when adding interfaces to a LAG:

- To determine the maximum number of LAG interfaces for your type of switch, look at the output from the **show capacities lag** command; however, the number of LAGs that can be created depends on the availability of the physical interface since each LAG interface needs at least one physical interface as a member link.
- After the maximum limit of members is reached in a LAG, an additional port cannot be added to the aggregation group. If a port belongs to a card type with a different speed than the other aggregation members, the port can still be added to the aggregation group. If dynamic LAG is enabled, any port member with a speed different than other aggregation members is blocked or ineligible from the same aggregation group. Any operational keys/attributes or configuration changes might affect the aggregation states of the member ports.
- The nondefaults configuration on an interface is removed automatically when the interface is added to a link aggregation. For example: Assume that you remove a member interface from an existing LAG and add it to another LAG. The software removes the nondefault configurations on the interface when it is added to the new LAG.

Examples

Creating a Link Aggregation Group (LAG) interface represented by an ID of 100:

```
switch(config)# interface lag 100
```

Deleting a Link Aggregation Group (LAG) interface represented by an ID of 100:

```
switch(config)# no interface lag 100
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

interface persona lag

```
interface persona lag <NAME>
no interface persona lag <NAME>
```

Description

Creates a persona LAG, a template for LAG (Link Aggregation Group) interfaces. A persona LAG defines configuration options that can be applied to multiple LAGs for consistency and simplified management. Only LAG interfaces can reference persona LAG templates. The persona LAG name cannot use reserved interface names or formats, such as vlan, lag, or loopback. Configurations defined in a persona LAG are valid only for LAG interfaces.

The **no** form of this command deletes the persona LAG interface.

Parameter	Description
<NAME>	Specifies the name of the persona LAG.

Usage

Keep in mind the following requirements when adding interfaces to a LAG:

- Persona LAG names must not match reserved interface names or formats (e.g., vlan, lag, loopback).
- Only LAG interfaces can use persona LAGs.
- Configuration applied to a persona LAG is only applicable to LAG interfaces.
- The persona LAG name is case-sensitive and can contain up to 54 characters.
- Names can include any characters, but avoid spaces or characters that may interfere with CLI parsing.
- Multi-chassis LAG interfaces do not support personas.

Examples

Creating a persona LAG template:

```
switch(config)# interface persona lag server-uplink
switch(config-persona-lag)# no shutdown
switch(config-persona-lag)# mtu 9000
switch(config-persona-lag)# description "Server uplink template"
```

Deleting a persona LAG template:

```
switch(config)# no interface persona lag server-uplink
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ip address

```
ip address <IPV4-ADDR>/<MASK> [secondary]
no ip address <IPV4-ADDR>/<MASK> [secondary]
```

Description

Sets an IPv4 address and subnet mask to a LAG interface. One primary and up to 31 secondary address can be configured per interface.

The **no** form of this command removes the IPv4 address from the interface.

Parameter	Description
<IPV4-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100 .
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.
secondary	Specifies a secondary IP address.

Examples

Setting an IP address on the LAG interface 1 to 198.51.100.1 with a mask of 24 bits:

```
switch(config)# interface lag 1
switch(config-lag-if)# ip address 198.51.100.1/24
```

Removing the IP address 198.51.100.1 with a mask of 24 bits from LAG interface 1:

```
switch(config)# interface lag 1
switch(config-lag-if)# no ip address 198.51.100.1/24
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 address

```
ipv6 address <IPV6-ADDR>/<MASK>  
no ipv6 address <IPV6-ADDR>/<MASK>
```

Description

Sets an IPv6 address and subnet mask to a LAG interface.

The **no** form of this command removes the IPv6 address from the interface.

Parameter	Description
<IPV6-ADDR>	Specifies the IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. You can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a quartet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

Setting the IPv6 address on LAG interface 1 to 2001:0db8:85a3::8a2e:0370:7334 with a mask of 24 bits:

```
switch(config)# interface lag 1  
switch(config-lag-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
```

Removing the IP address 2001:0db8:85a3::8a2e:0370:7334 with mask of 24 bits with a mask of 24 bits from LAG interface 1:

```
switch(config)# interface lag 1  
switch(config-lag-if)# no ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-lag-if	Administrators or local user group members with execution rights for this command.

lacp fallback

lacp fallback
no lacp fallback

Description

Configures the LACP fallback on LAG port.

The no form of this command sets the LAG to BLOCK state if no LACP partner is detected.

Usage

This makes members of the LAG function as non-bonded interfaces when no LACP partner is detected. This configuration is only applicable when the LAG is of type MCLAG. If the member port does not get an LACP frame, the port is in IE state.

Examples

Configuring LACP fallback on LAG port.

```
switch(config)# int lag 1 multi-chassis
switch(config-lag-if)# no sh
switch(config-lag-if)# lacp mode active
switch(config-lag-if)# lacp fallback
```

Configuring the LAG to BLOCK state when no LACP partner is detected.

```
switch(config)# int lag 1 multi-chassis
switch(config-lag-if)# no sh
switch(config-lag-if)# lacp mode active
switch(config-lag-if)# no lacp fallback
```

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.
9300S	config-lag-if	

lacp fallback-static

```
lacp fallback-static
no lacp fallback-static
```

Description

Configures the LACP fallback-static on LAG port.

The no form of this command sets the LAG to BLOCK state if no LACP partner is detected.

Usage

This makes members of the LAG function as non-bonded interfaces when no LACP partner is detected. One member interface that is part of the LAG stays up and forwards traffic, while the other members are in lacp-block state. This configuration is applicable when the lag is of type LACP and ignored in other cases. When this command is configured, only one member of LAG is selected to be UP. Enabling multiple members results in configuration mismatch on peer, loop, mac-learning issues, and more.

Examples

Configuring LACP fallback-static on LAG port.

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp mode active
switch(config-lag-if)# lacp fallback-static
```

Configuring the LAG to BLOCK state when no LACP partner is detected.

```
switch(config)# interface lag 1
switch(config-lag-if)# no lacp fallback-static
```

Configuring LACP fallback-static on static port.

```
switch(config-lag-if)# lacp fallback-static
Cannot enable LACP fallback-static on static LAG.
```

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-if config-lag-if	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

lacp hash

```
lacp hash [l2-src-dst | l3-src-dst | l4-src-dst]
no lacp hash [l2-src-dst | l3-src-dst | l4-src-dst]
```

Description

Controls the selection of an interface in a group of aggregate interfaces. The hash type value helps transmit a frame. This configuration must be done at the global level.

Parameter	Description
l2-src-dst	Specifies the load-balancing calculation to include only layer 2 items, such as source and destination MAC addresses.
l3-src-dst	Specifies the load-balancing calculation to include only layer 3 items, such as source and destination IP addresses.
l4-src-dst	Specifies the load-balancing calculation to include only layer 4 items, such as source and destination UDP/TCP ports.

Example

```
switch(config)# lacp hash l2-src-dst
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config	Administrators or local user group members with execution rights for this command.

lacp mode

```
lacp mode {active | passive}
no lacp mode {active | passive}
```

Description

Sets an LACP mode to active or passive.

The **no** form of this command sets the LACP mode to **off**, returning the LAG to a static mode aggregation.

Parameter	Description
active	Specifies that the local switch will transmit LACP Data Units (LACPDUs) to attempt to negotiate with the remote device.
passive	Specifies that the local switch will listen for LACPDUs from the remote device for LACP negotiation. NOTE: A momentary traffic drop occurs because LACP partners reconverge when changing the mode from active to passive or from passive to active.

Examples

Setting the LACP mode to `active`:

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp mode active
```

Setting the LACP mode to `off`:

```
switch(config)# interface lag 1
switch(config-lag-if)# no lacp mode active
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-lag-if	Administrators or local user group members with execution rights for this command.

lacp port-id

```
lacp port-id <PORT-ID>
no lacp port-id
```

Description

Sets the LACP port ID value of the member interface of the LAG.

The **no** form of this command removes the LACP port ID value from the interface.

Parameter	Description
<i><PORT-ID></i>	Specifies a port ID value. Range: 1 to 65535.

Examples

Setting an LACP port ID to a value of 10:

```
switch(config-if) # lacp port-id 10
```

Removing the LACP port ID value:

```
switch(config-if) # no lacp port-id
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

lacp port-priority

```
lacp port-priority <PORT-PRIORITY>  
no lacp port-priority
```

Description

Sets an LACP port priority value for the member interface of the LAG.

The **no** form of this command reverts the LACP port priority to the default, which is 1.

Parameter	Description
<i><PORT-PRIORITY></i>	Specifies a port priority value. Range: 1 to 65535.

Examples

Setting a LACP port priority value of 10:

```
switch(config-if)# lacp port-priority 10
```

Reverting the LACP port ID to the default:

```
switch(config-if)# no lacp port-priority
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

lacp rate

```
lacp rate {fast | slow}  
no lacp rate {fast | slow}
```

Description

Sets an LACP heartbeat request time to fast or slow.

The **no** form of the command sets an LACP rate to **slow**.

Parameter	Description
fast	Specifies the heartbeat request to every second, and the timeout period is a three-consecutive heartbeat loss that is 3 seconds.
slow	Specifies the heartbeat request to every 30 seconds. The timeout period is three-consecutive heartbeat loss that is 90 seconds. Default setting.

Examples

Setting the LACP heartbeat request time to *fast*:

```
switch(config)# interface lag 1  
switch(config-lag-if)# lacp rate fast
```

Resetting the LACP heartbeat request time to the default, which is `slow`:

```
switch(config)# interface lag 1
switch(config-lag-if)# no lacp rate
```

Another way to set the LACP heartbeat request time to the default, which is `slow`:

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp rate slow
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-lag-if	Administrators or local user group members with execution rights for this command.

lacp system-priority

```
lacp system-priority <SYSTEM-PRIORITY-VALUE>
no lacp system-priority <SYSTEM-PRIORITY-VALUE>
```

Description

Sets a Link Aggregation Control Protocol (LACP) system priority.
The **no** form of this command sets an LACP system priority to the default, which is 65534.

Parameter	Description
<SYSTEM-PRIORITY-VALUE>	Specifies a system priority value. Range: 0 to 65535.

Examples

Setting a Link Aggregation Control Protocol (LACP) system priority to 100:

```
switch(config)# lacp system-priority 100
```

Setting an LACP system priority to the default (65534):

```
switch(config)# no lacp system-priority
```

A momentary traffic drop can be seen in case the LACP state machine must renegotiate.



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lag

```
lag <ID>
no lag <ID>
```

Description

Adds an interface to a specified LAG interface ID.

The **no** form of this command removes an interface from a specified LAG interface ID. The member loses its LACP configuration when removed from the LAG. The member also reaches the default state with an administrative shutdown. For 6300 and 6400 series switches, the administrative state is enabled. Configurations, such as MTU and UDLD, are retained.

Parameter	Description
<ID>	Specifies a LAG interface ID. Range: 1 to 256.

Usage

- All members of the LAG must have the same speed. If a member comes up late with a different speed, it will not participate in the LAG/LACP. The hardware restriction is applied before adding an interface to LAG. The member belongs to the card type that has the same maximum speed as the reference port card type.
- To move an interface from LagA to LagB, first remove the interface from LagA and then add it to LagB. When a member is attached to a LAG, the nondefault configurations on the member are removed silently.
- After removing a physical interface from a LAG, the interface associated with the LAG becomes L3 ports with default L3 configurations and administrative down. For example, suppose interface 1/1/1 was part of LAG 3 and you had administratively enabled the interface. If you later remove interface 1/1/1 from LAG 3, the administrative status automatically changes to down. If you want to use the interface again, you must administratively enable it again.

Examples

Adding an interface to a Link Aggregation Group (LAG) represented by an ID of 100:

```
switch(config)# interface 1/1/1
switch(config-if)# lag 100
```

Deleting an interface from a Link Aggregation Group (LAG) represented by an ID of 100:

```
switch(config)# interface 1/1/1
switch(config-if)# no lag 100
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

persona custom

```
persona custom <NAME> {copy | attach}
no persona custom <NAME> {copy | attach}
```

Description

Assigns a persona LAG (Link Aggregation Group) to a LAG interface. The persona LAG is used to apply a common configuration to multiple LAGs. There are two modes for applying a persona LAG: **copy** and **attach**.

The **no** form of this command deletes the persona LAG.

Parameter	Description
<NAME>	Specifies the custom interface persona name. Range: 1 to 54 characters.
copy	Performs a one-time copy of the template LAG configuration. Subsequent changes to the template are not applied. If the specified persona LAG does not exist, the system displays the message persona LAG <name> not found .
attach	Performs an initial copy of the template LAG configuration, and

Parameter	Description
	any subsequent changes to the template are automatically applied to all attached LAGs. The template LAG does not need to exist before other LAGs are attached to it. After attachment, the copied settings can be modified on an individual LAG. However, any later change to the template overwrites the modified values with the updated template values. Existing LAG configuration prior to attachment is discarded and is not restored if the template is removed.

Usage

Keep in mind the following when assigning a persona LAG:

- Only LAG interfaces can be assigned a persona LAG.
- Physical interfaces cannot be assigned a persona LAG.
- When using the **copy** option, the persona LAG must exist before it can be used; for the **attach** option, it is created if it does not already exist.
- If a persona LAG is deleted, all LAGs referencing it retain their last applied settings.
- LAG configuration that existed prior to attaching a persona LAG is discarded and is not restored if the template is removed.
- When using the **attach** option, changes to the persona LAG template are immediately applied to all attached LAGs.

Examples

Creating a persona LAG template and assigning it to a LAG with the **attach** option:

```
switch(config)# interface persona lag server-uplink
switch(config-persona-lag)# mtu 9000
switch(config-persona-lag)# description "Server uplink LAG"
switch(config-persona-lag)# exit
switch(config)# interface lag 10
switch(config-lag-if)# persona custom server-uplink attach
```

Creating a persona LAG template and assigning it to a LAG with the **copy** option:

```
switch(config)# interface persona lag server-uplink
switch(config-persona-lag)# mtu 9000
switch(config-persona-lag)# description "Server uplink LAG"
switch(config-persona-lag)# exit
switch(config)# interface lag 11
switch(config-lag-if)# persona custom server-uplink copy
switch(config-lag-if)# end
```

Removing a persona LAG from a LAG:

```
switch(config)# interface lag 11
switch(config-lag-if)# no persona custom server-uplink attach
```

Removing a persona LAG assignment completely:

```
switch(config)# interface lag 11
switch(config-lag-if)# no persona custom server-uplink
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-lag-if	Administrators or local user group members with execution rights for this command.

show interface

```
show interfaces <LAG-NAME> [vsx-peer]
```

Description

Displays information about a specific LAG.

Parameter	Description
<LAG-NAME>	Specifies a LAG name.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying information about LAG 100:

```
switch# show interface lag100
Aggregate lag100 is up
Admin state is up
Description :
MAC Address      : 48:0f:cf:af:43:9c
Aggregated-interfaces : 1/1/2
Aggregation-key   : 100
Aggregate mode    : active
Speed             : 2000 Mb/s
L3 Counters: Rx Disabled, Tx Disabled
qos trust none
VLAN Mode: access
```

Access VLAN: 1

Statistics	RX	TX	Total
Packets	20	45	65
Unicast	5	5	10
Multicast	5	15	20
Broadcast	10	25	35
Bytes	5658	2584	8242
Jumbos	0	0	0
Dropped	0	0	0
Filtered	0	0	0
Pause Frames	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface persona

show interface persona

Description

Shows all interface personas and their attached interfaces.

Examples

Showing all interface personas and their attached interfaces:

```
switch(config)# show interface persona
-----
Persona          Type          Attached Interfaces
-----
access           physical      1/1/1
personal         physical      1/1/1-1/1/2
```

```
persona2      physical      --
access_lag    lag          lag20, lag30
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.17	Added support for persona LAG interfaces.
10.12	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show lacp aggregates

```
show lacp aggregates [<LAG-NAME>] [vsx-peer]
```

Description

Displays all LACP aggregate information configured for all LAGs, or for a specific LAG.

Parameter	Description
<LAG-NAME>	Optional: Specifies a lag name.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying LACP aggregate information configured for lag10:

```
switch# show lacp aggregates lag10

Aggregate-name       : lag10
Aggregated-interfaces : 1/1/1 1/1/2
Heartbeat rate       : slow
Hash                  : 13-src-dst
Aggregate mode        : active
```

Displaying LACP aggregates:

```
switch# show lacp aggregates

Aggregate-name      : lag1
Aggregated-interfaces : 1/1/27 1/1/28 1/1/29
Heartbeat rate      : slow
Hash                : 13-src-dst
Aggregate mode      : active

Aggregate-name      : lag2
Aggregated-interfaces : 1/1/48
Heartbeat rate      : slow
Hash                : 12-src-dst
Aggregate mode      : passive
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lacp configuration

show lacp configuration [vsx-peer]

Description

Displays global LACP configuration.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying global LACP configuration:

```
switch# show lacp configuration
System-id      : 98:f2:b3:68:40:a0
System-priority : 65534
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lacp interfaces

```
show lacp interfaces [<IFNAME>] [vsx-peer]
```

Description

Displays an LACP configuration of the physical interfaces, including VSXs. If an interface name is passed as argument, it only displays an LACP configuration of a specified interface.

Parameter	Description
<IFNAME>	Optional: Specifies an interface name.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

This example displays an LACP configuration of the physical interfaces. One of the interfaces has the **lacp-block** forwarding state. If a VSX switch has loop protect enabled on an interface and a loop occurs, VSX blocks the interface to stop the loop. The forwarding state of the blocked interface is set to **lacp-block**.

```
switch# show lacp interfaces
State abbreviations :
A - Active           P - Passive           F - Aggregable I - Individual
S - Short-timeout    L - Long-timeout  N - InSync      O - OutofSync
C - Collecting       D - Distributing
```

X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

--								
Intf	Aggr name	Port id	Port Pri	State	System-id	System Pri	Aggr Key	Forwarding State

--								
1/1/1	lag10	17	1	ALFOE	70:72:cf:37:a3:5c	20	10	lACP-block
1/1/2	lag128	69	1	ALFNCD	70:72:cf:37:a3:5c	20	128	up
1/1/3	lag128	14	1	ALFNCD	70:72:cf:37:a3:5c	20	128	up
1/1/4	lag128							down
1/1/5	lag20							up

Partner details of all interfaces:

Intf	Aggr name	Partner Port-id	Port Pri	State	System-id	System Priority	Aggr Key	

1/1/1	lag10	0	65534	PLFOEX	00:00:00:00:00:00	65534	0	
1/1/2	lag128	69	1	PLFNCD	70:72:cf:8c:60:a7	65534	128	
1/1/3	lag128	14	1	PLFNCD	70:72:cf:8c:60:a7	65534	128	
1/1/4	lag128							
1/1/5	lag20							

Displaying static LAG:



lACP fallback-static cannot be configured on static lag. Attempts to configure **lACP fallback-static** on a static LAG results in the following message:

Cannot enable LACP-fallback static on static LAG.

switch# **show lacp interfaces**

State abbreviations :

A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-id	System Pri	Aggr Key	Forwarding State

1/1/1	lag10							up
1/1/2	lag10							up

Partner details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-id	System Pri	Aggr Key	

1/1/1	lag10							
1/1/2	lag10							

State abbreviations :

A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-id	System Pri	Aggr Key	Forwarding State
1/1/1	lag10							up
1/1/2	lag10							up

Partner details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-id	System Pri	Aggr Key
1/1/1	lag10						
1/1/2	lag10						

Displaying an LACP configuration of the 1/1/1 interface:

```
switch# show lacp interfaces 1/1/1
```

State abbreviations :

A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Aggregate-name : lag1

	Actor	Partner
Port-id	28	31
Port-priority	1	1
Key	1	1
State	ALFNCD	ALFNCD
System-id	98:f2:b3:68:40:a0	98:f2:b3:68:60:a6
System-priority	65534	65534

Displaying an LACP configuration after loop-protect is enabled on the primary VSX switch:

```
switch# show lacp interfaces
```

State abbreviations :

A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

Intf	Aggr Name	Port Id	Port Pri	State	System-ID	System Pri	Aggr Key	Forwarding State
1/4/14	lag1(mc)	206	1	ALFNCD	f8:60:f0:06:49:00	65534	1	up
1/5/15	lag2(mc)							down

Partner details of all interfaces:


```

-----
Intf      Aggr      Port  Port  State  System-ID          System Aggr
Name      Id    Pri                    Pri    Key
-----
1/4/14    lag1(mc)   130   1      ALFNCD f8:60:f0:06:87:00 65534  1
1/5/15    lag2(mc)

```

Displaying an LACP configuration after loop-protect is enabled on the secondary VSX switch:

```

switch# show lacp interfaces

State abbreviations :
A - Active          P - Passive          F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync      O - OutofSync
C - Collecting      D - Distributing
X - State m/c expired      E - Default neighbor state

Actor details of all interfaces:
-----
Intf      Aggr      Port  Port  State  System-ID          System Aggr Forwarding
Name      Id    Pri                    Pri    Key    State
-----
1/3/2     lag1(mc)   1130  1      ALFNCD f8:60:f0:06:49:00 65534  1    up
1/9/3     lag2(mc)
                                     down

Partner details of all interfaces:
-----
Intf      Aggr      Port  Port  State  System-ID          System Aggr
Name      Id    Pri                    Pri    Key
-----
1/3/2     lag1(mc)   131   1      ALFNCD f8:60:f0:06:87:00 65534  1
1/9/3     lag2(mc)

```

Displaying an LACP configuration with LACP fallback:

```

switch# show lacp interfaces

State abbreviations :
A - Active          P - Passive          F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync      O - OutofSync
C - Collecting      D - Distributing
X - State m/c expired      E - Default neighbor state

Actor details of all interfaces:
-----
Intf      Aggr      Port  Port  State  System-ID          System Aggr Forwarding
Name      Id    Pri                    Pri    Key    State
-----
1/1/4     lag10      5     1      IE     ec:eb:b8:e4:29:00 65534  10    up
1/1/5     lag10      6     1      IE     ec:eb:b8:e4:29:00 65534  10    lacp-block
1/1/6     lag10      7     1      IE     ec:eb:b8:e4:29:00 65534  10    lacp-block
1/3/27    lag10     156   1      IE     ec:eb:b8:e4:29:00 65534  10    lacp-block
1/1/9     lag20(mc)  9     1      IE     ec:eb:b8:e4:29:00 65534  10    up

Partner details of all interfaces:
-----
Intf      Aggr      Port  Port  State  System-ID          System Aggr
Name      Id    Pri                    Pri    Key
-----

```

```

-----
1/1/4      lag10      0      0      IE      00:00:00:00:00:00 0      0
1/1/5      lag10      0      0      IE      00:00:00:00:00:00 0      0
1/1/6      lag10      0      0      IE      00:00:00:00:00:00 0      0
1/3/27     lag10      0      0      IE      00:00:00:00:00:00 0      0
1/1/9      lag20 (mc) 0      0      IE      00:00:00:00:00:00 0      0

```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.11	LACP fallback-static added.
10.11	LACP fallback added on VSX-supported platforms.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lag

`show lag <LAG-ID>`

Description

Displays the lag.

Parameter	Description
<LAG-ID>	Specifies the lag ID.

Examples

Displaying the lag.

```

switch# show lag

System-ID      : f4:03:43:80:4a:00
System-priority : 65534
Hash           : 13-src-dst
Aggregate lag1 is down
  Admin state is down
  Description :

```

```

Type                : normal
Lacp Fallback       : n/a
MAC Address         : f4:03:43:80:4a:00
Aggregated-interfaces :
Aggregation-key     : 1
Aggregate mode      : static
LACP rate           : n/a
Speed               : 0 Mb/s
Mode                : routed

Aggregate lag128 is down
Admin state is down
Description :
Type                : normal
Lacp Fallback       : n/a
MAC Address         : f4:03:43:80:4a:00
-- MORE --, next page: Space, next line: Enter, quit: q

```

Displaying the lag when lacp fallback-static is enabled.

```

switch# show lag

System-ID          : 90:20:c2:24:60:00
System-priority    : 65534

Aggregate lag1 is up
Admin state is up
Description :
Type                : normal
Lacp Fallback       : Enabled
MAC Address         : 90:20:c2:24:60:00
Aggregated-interfaces : 1/1/1 1/1/2 1/1/3 1/1/46 1/1/47 1/1/48
Aggregation-key     : 1
Aggregate mode      : active
Hash                : 13-src-dst
LACP rate           : slow
Speed               : 1000 Mb/s
Mode                : trunk

```

Release	Modification
10.11	LACP fallback-static added.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config interface

show running-config interface

[IFNAME | IFRANGE | lag <LAGNUM.ID> | loopback <NUMBER> | mgmt | persona | tunnel <ID> | vlan <ID> | vsx-peer | vxlan] {vsx-peer}

Description

Displays the running configuration for the interface.

Parameter	Description
<IFNAME>	Displays the interface name.
<IFRANGE>	Displays the PORT identifier range.
lag <LAGNUM.ID>	Displays the LAG interface information. Range: 1 to 4094.
loopback <NUMBER>	Displays the loopback interface information. Range: 0 to 255.
mgmt	Displays the management interface information.
persona	Displays the interface persona information.
tunnel <ID>	Displays the tunnel interface information. Range: 1 to 1255. ▪ gre ip: Displays the details of GRE IPv4 tunnel interface. ▪ ip 6in4: Displays the details of IPv6 in IPv4 tunnel information. ▪ ip 6in6: Displays the details of IPv6 in IPv6 tunnel information.
vlan <ID>	Displays the VLAN interface information. Range: 1 to 4094.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.
vxlan	Displays the VXLAN interface information. Default: 1.

Examples

Displaying the running configuration for the interface.

```
switch# show running-config interface
interface lag 10
  no shutdown
  mtu 9000
  description "Server uplink LAG"
  persona custom server-uplink attach
interface lag 11
  no shutdown
  mtu 9000
  description "Server uplink LAG"
  persona custom server-uplink
interface persona lag server-uplink
  no shutdown
  mtu 9000
  description "Server uplink LAG"
```

Displaying the running configuration for interface lag.

```

switch# show running-config interface lag
interface lag 10 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 10-12
    lacp mode active
    exit
interface lag 11 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 10-12,2001
    lacp mode active
    exit
interface lag 256
    description VSX_ISL
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
    exit

```

Displaying the running configuration for interface lag with **lacp fallback-static** configured.

```

switch# show running-config interface lag
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
    lacp fallback-static

```

Displaying the running configuration for interface persona.

```

switch# show running-config interface persona
interface persona access
    shutdown
    no routing
    vlan access 1
    exit
interface persona personal
    shutdown
    no routing
    vlan access 1
    exit
interface persona persona2
    shutdown
    no routing
    vlan access 1
    exit

```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.17	Added support for persona LAG interfaces.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

shutdown

shutdown
no shutdown

Description

Sets every interface in the LAG operationally down.

The **no** form of this command sets every interface operationally up.

Examples

Setting every interface in the LAG to shutdown:

```
switch(config)# interface lag 1
switch(config-lag-if)#
```

Resetting every interface in the LAG to the default (up):

```
switch(config)# interface lag 1
switch(config-lag-if)# no shutdown
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-lag-if	Administrators or local user group members with execution rights for this command.

vlan trunk native

```
vlan trunk native <VLAN-ID>
no vlan trunk native [<VLAN-ID>]
```

Description

Assigns a native VLAN ID to a LAG interface.

The **no** form of this command removes a native VLAN from a LAG interface and assigns VLAN ID 1 as its native VLAN.

Parameter	Description
<VLAN-ID>	Specifies the number of the VLAN ID to assign. The VLAN ID must exist. Maximum number of VLANs supported: 4096 (9300/9300S) VLAN ID range: 2 to 4094.

Usage

By default, VLAN ID 1 is assigned as the LAG VLAN ID for all LAG interfaces. VLANs can only be assigned to a nonrouted (layer 2) interface or LAG interface.

Only one VLAN ID can be assigned as the native VLAN. For the interface to forward the native VLAN traffic, the interface has to be allowed explicitly by entering **vlan trunk allowed <ID>** where the ID is the native VLAN ID. This setting is also applicable to the physical interface.

Examples

Configuring a layer 2 dynamic aggregation group with native VLAN ID **1** assigned to LAG **1**:

For HPE Aruba Networking 6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300/9300S, and 10000 Switch series:

```
switch(config)# interface lag 1
switch(config-lag-if)# no shutdown
switch(config-lag-if)# no routing
switch(config-lag-if)# lacp mode active
switch(config-lag-if)# vlan trunk native 1
switch(config-lag-if)# vlan trunk allowed 1
```

Configuring a layer 2 dynamic aggregation group with native VLAN ID **20** assigned to LAG **1**:

For HPE Aruba Networking 6300, 6400, 8100, 8320, 8325, 8360, 8400, 9300/9300S, and 10000 Switch series:

```
switch(config)# interface lag 1
switch(config-lag-if)# no shutdown
switch(config-lag-if)# no routing
switch(config-lag-if)# lacp mode active
```

```
switch(config-lag-if)# vlan trunk native 20  
switch(config-lag-if)# vlan trunk allowed 20
```

Removing a native VLAN from LAG 1:

```
switch(config)# interface lag 1  
switch(config-lag-if)# no vlan trunk native
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

clear lldp neighbors

```
clear lldp neighbors
```

Description

Clears all LLDP neighbor details.

Examples

Clearing all LLDP neighbor details:

```
switch# clear lldp neighbors
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear lldp statistics

```
clear lldp statistics
```

Description

Clears all LLDP neighbor statistics.

Examples

Clearing all LLDP neighbor statistics:

```
switch# clear lldp statistics
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

lldp

```
lldp  
no lldp
```

Description

Enables LLDP support globally on all active interfaces. By default, LLDP is enabled.

The **no** form of this command disables LLDP support globally on all active interfaces. It does not remove any LLDP configuration settings.

Examples

Enabling LLDP:

```
switch(config)# lldp
```

Disabling LLDP:

```
switch(config)# no lldp
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp dot3

```
lldp dot3 {poe | macphy}  
no lldp dot3 {poe | macphy}
```

Description

Sets the 802.3 TLVs to be advertised. By default, advertisement of both POE and MAC/PHY TLVs is enabled. Not supported on the OOBM interface.

The **no** form of this command disables advertisement of 802.3 TLVs.

Parameter	Description
poe	Specifies advertisement of power over Ethernet data link classification.
macphy	Specifies advertisement of media access control and physical layer information.

Examples

Enabling advertisement of the POE TLV:

```
switch(config-if) # lldp dot3 poe
```

Disabling advertisement of the POE TLV:

```
switch(config-if) # no lldp dot3 poe
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

lldp dot3 mfs

```
lldp dot3 mfs
no lldp dot3 mfs
```

Description

Enables the 802.3 TLV list in LLDP to advertise for maximum frame size (MFS). Enabled by default. The **no** form of this command disables the advertisement of maximum frame size TLVs.

Examples

Enabling advertisement of maximum frame size TLVs:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp dot3 mfs
```

Disabling advertisement of maximum frame size TLVs:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp dot3 mfs
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp management-address vlan

```
lldp management-address vlan <VLAN-ID>
no lldp management-address vlan <VLAN-ID>
```

Description

Sets the VLAN whose IPv4 or IPv6 address is advertised as the LLDP management authority.

The **no** form of this command removes the VLAN whose IPv4 or IPv6 address is advertised as the LLDP management authority.

The following is the precedence for the management IP address TLV in the LLDP packet (in order):

- LLDP management-IP-address and management-ipv6-address, if configured.
- LLDP management VLAN's IPv4 and IPv6 address, if configured.
- Loopback IP address from the smallest configured loopback interface identifier.
- Route-only-port IP address (Layer-3 interface) or IP address of the SVI (Layer-2 interface).
- OOBM IP address.
- Base MAC address of the switch.

Parameter	Description
<VLAN-ID>	Specifies the VLAN ID.

Examples

Setting the management authority for VLAN 10:

```
switch(config)# lldp management-address vlan 10
```

Removing the management authority for VLAN 10:

```
switch(config)# no lldp management-address vlan 10
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp management-ip-address

```
lldp management-ip-address <IPV-ADDR>  
no lldp management-ip-address
```

Description

Defines the IP management address of the switch which is sent in the management address TLV. One IPv4 and one IPv6 management address can be configured.

If you do not define an LLDP management address, then LLDP uses one of the following (in order):

- IP address of the port
- IP address of the management interface
- Base MAC address of the switch

The **no** form of this command removes the IPv4 management address of the switch.

Parameter	Description
<code><IPV4-ADDR></code>	Specifies the management address of the switch as an IPv4 format (x.x.x.x), where x is a decimal value from 0 to 255.

Examples

Setting the management address to **10.10.10.2**:

```
switch(config)# lldp management-ip-address 10.10.10.2
```

Removing the management address:

```
switch(config)# no lldp management-ip-address
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14	The management-ipv4-address keyword is deprecated and replaced with management-ip-address .
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

lldp management-ipv6-address

```
lldp management-ipv6-address <IPV6-ADDR>  
no lldp management-ipv6-address
```

Description

Defines the IPv6 management address of the switch. The management address is encapsulated in the management address TLV.

If you do not define an LLDP management address, then LLDP uses one of the following (in order):

- IP address of the port
- IP address of the management interface
- Base MAC address of the switch

The **no** form of this command removes the IPv6 management address of the switch.

Parameter	Description
<code><IPV6-ADDR></code>	Specifies an IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

Examples

Setting the management address to 2001:db8:85a3::8a2e:370:7334:

```
switch(config)# lldp management-ipv6-address 2001:0db8:85a3::8a2e:0370:7334
```

Removing the management address:

```
switch(config)# no lldp management-ipv6-address
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp med

```
lldp med [poe [priority-override] | capability | network-policy]  
no med [poe [priority-override] | capability | network-policy]
```

Description

Configures support for the LLDP-MED TLV. LLDP-MED (media endpoint devices) is an extension to LLDP developed by TIA to support interoperability between VoIP endpoint devices and other networking end-devices. The switch only sends the LLDP MED TLV after receiving a MED TLV from and connected endpoint device.

Not supported on the OOBM interface.

The **no** form of this command disables support for the LLDP MED TLV.

Parameter	Description
<code>poe [priority-override]</code>	Specifies advertisement of power over Ethernet data link classification. The priority-override option overrides user-configured port priority for Power over Ethernet. When both lldp dot3 poe and lldp med poe are enabled, the lldp dot3 poe3 setting takes precedence. Default: enabled.
<code>capability</code>	Specifies advertisement of supported LLDP MED TLVs. The capability TLV is always sent with other MED TLVs, therefore it cannot be disabled when other MED TLVs are enabled. Default: enabled.
<code>network-policy</code>	Network policy discovery lets endpoints and network devices advertise their VLAN IDs, and IEEE 802.1p (PCP and DSCP) values for voice applications. This TLV is only sent when a voice VLAN policy is present. Default: enabled.

Examples

Enabling advertisement of the network policy TLV:

```
switch(config-if) # lldp med network-policy
```

Disabling advertisement of the network policy TLV:

```
switch(config-if) # no lldp med network-policy
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Administrators or local user group members with execution rights for this command.

lldp med location

```
lldp med location {civic-addr  elin-addr }  
no med location {civic-addr  elin-addr }
```

Description

Configures support for the LLDP-MED TLV. Supports only civic address and emergency location information number (ELIN). Coordinate-based location is not supported.

The **no** form of this command disables support for the LLDP MED TLV.

Parameter	Description
civic-addr	Configures the LLDP MED civic location TLV.
elin-addr	Configures support for the LLDP MED emergency location TLV. This feature is intended for use in ECS applications to support class 3 LLDP-MED VoIP telephones connected to a switch in an MLTS infrastructure. An ELIN is a valid NANP format telephone number assigned to MLTS operators in North America by the appropriate authority. The ELIN is used to route emergency (E911) calls to a PSAP. (Range: 1-15 numeric characters)

The **lldp med location civic-addr** command requires a minimum of one type/value pair, but typically includes multiple type/value pairs as needed to configure a complete set of data describing a given location.

CA-TYPE: This is the first entry in a type/value pair and is a number defining the type of data contained in the second entry in the type/value pair (CA-VALUE.) Some examples of CA-TYPE specifiers include: 3=city 6=street (name) 25=building name (Range: 0 - 255)

CA-VALUE: This is the second entry in a type/value pair and is an alphanumeric string containing the location information corresponding to the immediately preceding CA-TYPE entry. Strings are delimited by either blank spaces, single quotes (' ... '), or double quotes ("... "). Each string should represent a specific data type in a set of unique type/value pairs comprising the description of a location, and each string must be preceded by a CA-TYPE number identifying the type of data in the string.

The following LLDP-MED TLV values are supported. For details on these value types, refer to [RFC 4776](#)

- 1: national subdivisions (state, canton, region, province, prefecture)
- 2: county, parish, gun (JP), district (IN)
- 3: city, township, shi (JP)
- 4: city division, borough, city district, ward, chou (JP)
- 5: neighborhood, block
- 6: group of streets below the neighborhood level
- 16: leading street direction N
- 17: trailing street suffix SW
- 18: street suffix or type
- 19: house number
- 20: house number suffix
- 21: landmark or vanity
- 22: location

- 23: name
- 24: postal/zip code
- 25: building (structure)
- 26: unit (apartment, suite)
- 27: floor
- 28: room
- 29: type of place
- 30: postal community name
- 31: post office box
- 32: additional code 13203000003
- 33: seat (desk, cubicle workstation)
- 34: primary road name 35 road section
- 36: branch road name
- 37: sub-branch road name
- 38: street name pre-modifier
- 39: street name post-modifier

Examples

Enabling support for the LLDP MED emergency location TLV:

```
switch(config-if)# lldp med location elin-addr 408-555-1212
```

Disabling support for the LLDP MED emergency location TLV:

```
switch(config-if)# no lldp med location elin-addr 408-555-1212
```

Enabling support for the LLDP MED civic address TLV:

```
switch(config-if)# lldp med location civic-addr US 1 19 123 6 Fake 18 Street
```

Disabling support for the LLDP MED civic address TLV:

```
switch(config-if)# no lldp med location civic-addr US 1 19 123 6 Fake 18 Street
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

lldp receive

```
lldp receive
no lldp receive
```

Description

Enables reception of LLDP information on an interface. By default, LLDP reception is enabled on all active interfaces, including the OOBM interface.

The **no** form of this command disables reception of LLDP information on an interface.

Examples

Enabling LLDP reception on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp receive
```

Disabling LLDP reception on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp receive
```

Enabling LLDP reception on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# lldp receive
```

Disabling LLDP reception on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# no lldp receive
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

lldp reinit

```
lldp reinit <TIME>
no lldp reinit
```

Description

Sets the amount of time (in seconds) to wait before performing LLDP initialization on an interface. The **no** form of this command sets the reinitialization time to its default value of 2 seconds.

Parameter	Description
<TIME>	Specifies the reinitialization time in seconds. Range: 1 to 10. Default: 2 seconds.

Examples

Setting the reinitialization time to 5 seconds:

```
switch(config)# lldp reinit 5
```

Setting the reinitialization time to the default value of 2 seconds:

```
switch(config)# no lldp reinit
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp select-tlv

```
lldp select-tlv <TLV-NAME>
no lldp select-tlv <TLV-NAME>
```

Description

Selects a TLV that the LLDP agent will send and receive. By default, all supported TLVs are sent and received.

The **no** form of this command stops the LLDP agent from sending and receiving a specific TLV.



LLDP supports Organization Unique Identifiers (OUIs) with the following Organization-specific TLVs:

- IEEE 802.1 (DOT1) (oui:0x00, 0x80, 0xc2)
- IEEE 802.3 (DOT3) (oui:0x00, 0x12, 0x0f)
- HPE Aruba Networking (oui:0x88, 0x3a, 0x30)

Parameter	Description
<code>select-tlv <TLV-NAME></code>	Specifies the TLV name to send. The following TLV names are supported: ▪ management-address: Selection is based on priority in the following list (for example if first TLV name isn't selected, the next will be, progressing through this list until a selection is made): 1. IPv4 or IPV6 management address. 2. IP address of the lowest configured loopback interface. 3. If layer 3, then the route-only port IP address. 4. If layer 2, the IP address of the SVI. 5. OOBM interface IP address. 6. Base MAC address of the switch. ▪ port-description: Select port-description TLV. ▪ port-vlan-id: Select port-vlan-id TLV. ▪ port-vlan-name: Select port-vlan-name TLV. ▪ system-capabilities: Select system-capabilities TLV. ▪ system-description: Select system-description TLV. ▪ system-name: Select system-name TLV.

Examples

Stopping the LLDP agent from sending the **port-description** TLV:

```
switch(config)# no lldp select-tlv port-description
```

Enabling the LLDP agent to send the **port-description** TLV:

```
switch(config)# lldp select-tlv oui
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp timer

```
lldp timer <TIME>  
no lldp timer
```

Description

Sets the interval (in seconds) at which local LLDP information is updated and TLVs are sent to neighboring network devices by the LLDP agent. The minimum setting for this timer must be four times the value of **lldp txdelay**.

For example, this is a valid configuration:

- **lldp timer** = 16
- **lldp txdelay** = 4

And, this is an invalid configuration:

- **lldp timer** = 5
- **lldp txdelay** = 2

When copying a saved configuration to the running configuration, the value for **lldp timer** is applied before the value of **lldp txdelay**. This can result in a configuration error if the saved configuration has a value of **lldp timer** that is not four times the value of **lldp txdelay** in the running configuration.

For example, if the saved configuration has the settings:

- **lldp timer** = 16
- **lldp txdelay** = 4



And the running configuration has the settings:

- **lldp timer** = 30
- **lldp txdelay** = 7

Then you will see an error indicating that certain configuration settings could not be applied, and you will have to manually adjust the value of **lldp txdelay** in the running configuration.

The **no** form of this command sets the update interval to its default value of 30 seconds.

Parameter	Description
<i><TIME></i>	Specifies the update interval (in seconds). Range: 5 to 32768. Default: 30.

Examples

Setting the update interval to 7 seconds:

```
switch(config)# lldp timer 7
```

Setting the update interval to the default value of 30 seconds:

```
switch(config)# no lldp timer
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp tlv-enable

```
lldp tlv-enable basic-tlv management-address-tlv {ip <X.X.X.X>}|{ipv6 <X:X::X:X>}
no lldp select-tlv <TLV-NAME>
```

Description

A **TLV** is an information element that contains the type, length, and value fields. This command configures the IPv4/IPv6 address to be advertised in the management address TLV. This configured value will take the highest precedence in the selection logic the switch uses to identify the IP address to be advertised in the management address TLV.

Parameter	Description
<i>ip <X.X.X.X></i>	Specify an IP address in IPv4 format (X.X.X.X), where X is a decimal number from 0 to 255.
<i>ipv6 <X:X::X:X></i>	Specify an IP address in IPv6 format (x:x::x:x), where X is a hexadecimal number from 0 to F .

Examples

Configuring an IP address in IPv4 format:

```
switch(config)# interface 1/3/1
switch(config-if)# lldp tlv-enable basic-tlv management-address-tlv ip 10.0.0.1
```

Configuring an IP address in IPv6 format:

```
switch(config)# interface 1/3/1
switch(config-if)# lldp tlv-enable basic-tlv management-address-tlv ipv6
2001:db8:85a3::8a2e:370:7334
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

lldp transmit

```
lldp transmit
no lldp transmit
```

Description

Enables transmission of LLDP information on specific interface. By default, LLDP transmission is enabled on all active interfaces, including the OOBM interface.

The **no** form of this command disables transmission of LLDP information on an interface.

Examples

Enabling LLDP transmission on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp transmit
```

Disabling LLDP transmission on interface **1/1/1**:


```
switch(config)# interface 1/1/1
switch(config-if)# no lldp transmit
```

Enabling LLDP transmission on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# lldp transmit
```

Disabling LLDP transmission on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# no lldp transmit
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

lldp txdelay

```
lldp txdelay <TIME>
no lldp txdelay
```

Description

Sets the amount of time (in seconds) to wait before sending LLDP information from any interface. The maximum value for **txdelay** is 25% of the value of **lldp tx timer**.

The **no** form of this command sets the delay time to its default value of 2 seconds.

Parameter	Description
<TIME>	Specifies the delay time in seconds. Range: 0 to 10. Default: 2.

Examples

Setting the delay time to 8 seconds:

```
switch(config)# lldp txdelay 8
```

Setting the delay time to the default value of 2 seconds:

```
switch(config)# no lldp txdelay
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp trap enable

```
lldp trap enable  
no lldp trap enable
```

Description

Enables sending SNMP traps for LLDP related events from a particular interface. LLDP trap generation is enabled by default on all the interfaces and has to be disabled for interfaces on which traps are not required to be generated.

The **no** form of this command disables the LLDP trap generation.



LLDP trap generation is disabled by default at the global level and must be enabled before any LLDP traps are sent.

Examples

Enabling LLDP trap generation on global level:

```
switch(config)# lldp trap enable
```

Enabling LLDP trap generation on interface level:

```
switch(config-if)# lldp trap enable
```

Disabling LLDP trap generation on global level:

```
switch(config)# no lldp trap enable
```

Disabling LLDP trap generation on interface level:

```
switch(config-if)# no lldp trap enable
```

Displaying LLDP global configuration:

```
switch# show lldp configuration
```

LLDP Global Configuration

=====

```
LLDP Enabled           : No
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : No
```

TLVs Advertised

=====

```
Management Address
Port Description
Port VLAN-ID
System Description
System Name
```

LLDP Port Configuration

=====

PORT	TX-ENABLED	RX-ENABLED	INTF-TRAP-ENABLED

1/1/1	Yes	Yes	Yes
1/1/2	Yes	Yes	Yes
1/1/3	Yes	Yes	Yes
1/1/4	Yes	Yes	Yes
1/1/5	Yes	Yes	Yes
1/1/6	Yes	Yes	Yes
.....			
.....			
mgmt	Yes	Yes	Yes

Displaying LLDP Configuration for the interface:

```
switch# show lldp configuration 1/1/1
```

LLDP Global Configuration

=====

```
LLDP Enabled           : Yes
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : No
```

```

LLDP Port Configuration
=====
PORT          TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-----
1/1/1         Yes                        Yes                  Yes

```

Displaying LLDP Configuration for the management interface:

```

switch# show lldp configuration mgmt

LLDP Global Configuration
=====
LLDP Enabled           : Yes
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : Yes

LLDP Port Configuration
=====
PORT          TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-----
mgmt          Yes                        Yes                  Yes

```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config and config-if	Administrators or local user group members with execution rights for this command.

show lldp configuration

```
show lldp configuration [<INTERFACE-ID>][vsx-peer]
```

Description

Shows LLDP configuration settings for all interfaces or a specific interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: member/slot/port .
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing configuration settings for all interfaces:

```
switch# show lldp configuration

LLDP Global Configuration
=====
LLDP Enabled           : No
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : No

TLVs Advertised
=====
Management Address
Port Description
Port VLAN-ID
System Description
System Name

LLDP Port Configuration
=====
PORT          TX-ENABLED      RX-ENABLED      INTF-TRAP-ENABLED
-----
1/1/1         Yes             Yes             Yes
1/1/2         Yes             Yes             Yes
1/1/3         Yes             Yes             Yes
1/1/4         Yes             Yes             Yes
1/1/5         Yes             Yes             Yes
1/1/6         Yes             Yes             Yes
.....
.....
mgmt          Yes             Yes             Yes
```

This example shows configuration settings for interface **1/1/1**.

```
switch# show lldp configuration 1/1/1

LLDP Global Configuration
=====
LLDP Enabled           : Yes
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : No
```

```

LLDP Port Configuration
=====
Auto Flush On Link Down      : Yes
Management IPv4 Address     : 10.1.1.1
Management IPv6 Address     : 3001:1::1:1
PORT          TX-ENABLED      RX-ENABLED      INTF-TRAP-ENABLED
-----
1/1/1          Yes            Yes            Yes

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	When displaying the LLDP configuration for a specific interface, the output of this command displays any configured management IP addresses.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp configuration mgmt

show lldp configuration mgmt

Description

Shows LLDP configuration settings for the OOBM interface.

Example

Showing configuration settings for all interfaces:

```

switch# show lldp configuration mgmt

LLDP Global Configuration
=====
LLDP Enabled              : Yes
LLDP Transmit Interval   : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled        : Yes

```

```

LLDP Port Configuration
=====
PORT                TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-----
mgmt                 Yes                  Yes                  Yes

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp local-device

```
show lldp local-device[vsx-peer]
```

Description

Shows global LLDP information advertised by the switch, as well as port-based data. If VLANs are configured on any active interfaces, the VLAN ID is only shown for trunk native or untagged VLAN IDs on access interfaces.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing global LLDP information only (all ports including OOBM port are administratively down):

```

switch# show lldp local-device

Global Data
=====

Chassis-ID           : 1c:98:ec:e3:45:00
System Name          : switch

```

```
System Description      : HPE ANW JL375A 8400X XL.01.01.0001
Management Address     : 192.168.10.1
Capabilities Available  : Bridge, Router
Capabilities Enabled    : Bridge, Router
TTL                    : 120
```

Showing all ports except **1/1/11** and OOBM as administratively down:

```
switch# show lldp local-device

Global Data
=====

Chassis-ID             : 1c:98:ec:e3:45:00
System Name            : switch
System Description     : HPE ANW
Management Address     : 192.168.10.1
Capabilities Available  : Bridge, Router
Capabilities Enabled    : Bridge, Router
TTL                    : 120

Port Based Data
=====

Port-ID                : 1/1/11
Port-Desc              : "1/1/11"
Port Mgmt-Address      : 164.254.21.220
Port VLAN ID           : 1

Port-ID                : mgmt
Port-Desc              : "mgmt"
Port Mgmt-Address      : 164.254.21.220
```

In this example, all the ports except **1/1/11** are administratively down, and VLAN ID 100 is configured on this access interface.

```
switch# show lldp local-device

Global Data
=====

Chassis-ID             : 1c:98:ec:e3:45:00
System Name            : switch
System Description     : HPE ANW
Management Address     : 192.168.10.1
Capabilities Available  : Bridge, Router
Capabilities Enabled    : Bridge, Router
TTL                    : 120

Port Based Data
=====

Port-ID                : 1/1/11
Port-Desc              : "1/1/11"
Port VLAN ID           : 100
Parent Interface       : interface 1/1/11
```




For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp neighbor-info

show lldp neighbor-info [<INTERFACE-NAME>] [vsx-peer]

Description

Displays information about neighboring devices for all interfaces or for a specific interface. The information displayed varies depending on the type of neighbor connected and the type of TLVs sent by the neighbor.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface for which to show information for neighboring devices. Use the format member/slot/port (for example, 1/3/1).
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing LLDP information for all interfaces:

```
switch# show lldp neighbor-info
```

```
LLDP Neighbor Information
=====
```

```
Total Neighbor Entries      : 3
Total Neighbor Entries Deleted : 0
Total Neighbor Entries Dropped : 0
Total Neighbor Entries Aged-Out : 0
```

```
LOCAL-PORT  CHASSIS-ID      PORT-ID      PORT-DESC      TTL      SYS-NAME
```

```

-----
1/1/1      70:72:cf:a4:7d:50  1/1/1      1/1/1      32      switch
1/1/2      48:0f:cf:af:73:80  1/1/2      1/1/2      120     switch
1/1/46     48:0f:cf:af:73:80  1/1/46     1/1/46     120     switch
mgmt       48:0f:cf:af:73:80  mgmt       mgmt       120     switch

```

Showing information for interface **1/3/1** when it has only one switch connected as a neighbor:

```

switch# show lldp neighbor-info 1/3/1

Port                : 1/1/1
Neighbor Entries    : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : HP-3800-24G-PoEP-2XG
Neighbor Chassis-Description : HP J9587A 3800-24G-PoE+-2XG Switch, revision...
Neighbor Chassis-ID : 10:60:4b:39:3e:80
Neighbor Management-Address : 192.168.1.1
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled : Bridge
Neighbor Port-ID : 1/1/1
Neighbor Port-Desc : 1/1/1
Neighbor Port VLAN ID : 1
Neighbor Port VLAN Name : DEFAULT_VLAN_1
Neighbor Port MFS : 1500
TTL : 120

```

Showing information for interface **1/3/10** when the neighbor sends a DOT3 power TLV:

```

switch# show lldp neighbor-info 1/3/10

Port                : 1/3/10
Neighbor Entries    : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : 84:d4:7e:ce:5d:68
Neighbor Chassis-Description : ArubaOS (MODEL: 325), Version HPE_ANW IAP
Neighbor Chassis-ID : 84:d4:7e:ce:5d:68
Neighbor Management-Address : 169.254.41.250
Chassis Capabilities Available : Bridge, WLAN
Chassis Capabilities Enabled : WLAN
Neighbor Port-ID : 84:d4:7e:ce:5d:68
Neighbor Port-Desc : eth0
TTL : 120
Neighbor Port VLAN ID : 1
Neighbor Port VLAN Name : DEFAULT_VLAN_1
Neighbor Port MFS : 1500
Neighbor PoE information : DOT3
Neighbor Power Type : TYPE2 PD
Neighbor Power Priority : Unkown
Neighbor Power Source : Primary
PD Requested Power Value : 25.0 W
PSE Allocated Power Value: 25.0 W
Neighbor Power Supported : Yes
Neighbor Power Enabled : Yes

```

```
Neighbor Power Class      : 5
Neighbor Power Paircontrol : No
PSE Power Pairs           : Signal
```

Showing information for interface **1/1/1** when it has multiple neighbors (displays a maximum of four):

```
switch# show lldp neighbor-info 1/1/1

Port                               : 1/1/1
Neighbor Entries                   : 4
Neighbor Entries Deleted           : 0
Neighbor Entries Dropped           : 0
Neighbor Entries Aged-Out          : 0
Neighbor Chassis-Name              : switch
Neighbor Chassis-Description       : hpe_anw JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID                : 1c:98:ec:fe:25:00
Neighbor Management-Address        : 10.1.1.2
Chassis Capabilities Available     : Bridge, Router
Chassis Capabilities Enabled       : Bridge, Router
Neighbor Port-ID                   : 1/1/1
Neighbor Port-Desc                 : 1/1/1
Neighbor Port VLAN ID              : 1
Neighbor Port VLAN Name            : DEFAULT_VLAN_1
Neighbor Port MFS                   : 1500
TTL                                : 120
Neighbor Chassis-Name              : switch
Neighbor Chassis-Description       : hpe_anw JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID                : 1c:98:ec:fe:25:01
Neighbor Management-Address        : 10.1.1.3
Chassis Capabilities Available     : Bridge, Router
Chassis Capabilities Enabled       : Bridge, Router
Neighbor Port-ID                   : 1/1/1
Neighbor Port-Desc                 : 1/1/1
Neighbor Port VLAN ID              : 1
Neighbor Port VLAN Name            : DEFAULT_VLAN_1
Neighbor Port MFS                   : 1500
TTL                                : 120
Neighbor Chassis-Name              : switch
Neighbor Chassis-Description       : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID                : 1c:98:ec:fe:25:02
Neighbor Management-Address        : 10.1.1.4
Chassis Capabilities Available     : Bridge, Router
Chassis Capabilities Enabled       : Bridge, Router
Neighbor Port-ID                   : 1/1/1
Neighbor Port-Desc                 : 1/1/1
Neighbor Port VLAN ID              : 50
Neighbor Port VLAN Name            : VLAN_50
Neighbor Port MFS                   : 1500
TTL                                : 120
Neighbor Chassis-Name              : switch
Neighbor Chassis-Description       : hpe_anw JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID                : 1c:98:ec:fe:25:03
Neighbor Management-Address        : 10.1.1.5
Chassis Capabilities Available     : Bridge, Router
Chassis Capabilities Enabled       : Bridge, Router
Neighbor Port-ID                   : 1/1/1
Neighbor Port-Desc                 : 1/1/1
Neighbor Port VLAN ID              : 100
Neighbor Port VLAN Name            : VLAN_100
```

```
Neighbor Port MFS      : 1500
TTL                    : 120
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp neighbor-info detail

```
show lldp neighbor-info detail [vsx-peer]
```

Description

Shows detailed LLDP neighbor information for all LLDP neighbor connected interfaces.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing detailed LLDP information for all interfaces:

```
switch# show lldp neighbor-info detail

LLDP Neighbor Information
=====

Total Neighbor Entries      : 6
Total Neighbor Entries Deleted : 2
Total Neighbor Entries Dropped : 0
Total Neighbor Entries Aged-Out : 2

-----
```

```

Port : 1/1/1
Neighbor Entries : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : 6300
Neighbor Chassis-Description : hpe_anw ...
Neighbor Chassis-ID : 38:11:17:1a:d5:00
Neighbor Management-Address : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled : Bridge, Router
Neighbor Port-ID : 1/1/4
Neighbor Port-Desc : 1/1/4
Neighbor Port VLAN ID : 1
Neighbor Port VLAN Name : DEFAULT_VLAN_1
Neighbor Port MFS : 1500
TTL : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported : true
Neighbor Auto-Neg Enabled : true
Neighbor Auto-Neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASE_TFD
Neighbor MAU type : 1000 BASE_TFD

```

```

-----

Port : 1/1/2
Neighbor Entries : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : 6300
Neighbor Chassis-Description : hpe_anw...
Neighbor Chassis-ID : 38:11:17:1a:d5:00
Neighbor Management-Address : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled : Bridge, Router
Neighbor Port-ID : 1/1/5
Neighbor Port-Desc : 1/1/5
Neighbor Port VLAN ID : 1
Neighbor Port VLAN Name : DEFAULT_VLAN_1
Neighbor Port MFS : 1500
TTL : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported : true
Neighbor Auto-Neg Enabled : true
Neighbor Auto-Neg Advertised : 1000 BASE_TFD, 100 BASE_T4, 10 BASE_TFD
Neighbor MAU type : 1000 BASE_TFD

```

```

-----

Port : 1/1/3
Neighbor Entries : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : 6300
Neighbor Chassis-Description : hpe_anw ...
Neighbor Chassis-ID : 38:11:17:1a:d5:00
Neighbor Management-Address : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router

```

```

Chassis Capabilities Enabled : Bridge, Router
Neighbor Port-ID             : 1/1/6
Neighbor Port-Desc           : 1/1/6
Neighbor Port VLAN ID        : 1
Neighbor Port VLAN Name      : DEFAULT_VLAN_1
Neighbor Port MFS             : 1500
TTL                           : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported   : true
Neighbor Auto-Neg Enabled     : true
Neighbor Auto-Neg Advertised  : 1000 BASE_TFD, 100 BASE_T4, 10 BASE_TFD
Neighbor MAU type             : 1000 BASE_TFD

```

```

-----

Port                           : 1/1/46
Neighbor Entries               : 1
Neighbor Entries Deleted       : 0
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 0
Neighbor Chassis-Name          : 6300
Neighbor Chassis-Description   : hpe_anw ...
Neighbor Chassis-ID            : 38:11:17:1a:d5:00
Neighbor Management-Address    : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/19
Neighbor Port-Desc             : 1/1/19
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
TTL                            : 120

```

```

Neighbor Mac-Phy details
Neighbor Auto-neg Supported     : true
Neighbor Auto-Neg Enabled       : true
Neighbor Auto-Neg Advertised    : 1000 BASE_TFD, 100 BASE_T4, 10 BASE_TFD
Neighbor MAU type               : 1000 BASE_TFD

```

```

-----

Port                           : 1/1/47
Neighbor Entries               : 1
Neighbor Entries Deleted       : 0
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 0
Neighbor Chassis-Name          : 6300
Neighbor Chassis-Description   : hpe_anw ...
Neighbor Chassis-ID            : 38:11:17:1a:d5:00
Neighbor Management-Address    : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp neighbor-info mgmt

show lldp neighbor-info mgmt

Description

Displays information about neighboring devices connected to the OOBM interface.

Examples

Showing LLDP information for the OOBM interface:

```
switch# show lldp neighbor-info mgmt

Port                               : mgmt
Neighbor Entries                   : 1
Neighbor Entries Deleted           : 0
Neighbor Entries Dropped           : 0
Neighbor Entries Aged-Out          : 0
Neighbor Chassis-Name              : HP-3800-24G-PoEP-2XG
Neighbor Chassis-Description       : HP J9587A 3800-24G-PoE+-2XG Switch, revision...
Neighbor Chassis-ID                : 10:60:4b:39:3e:80
Neighbor Management-Address        : 192.168.1.1
Chassis Capabilities Available     : Bridge, Router
Chassis Capabilities Enabled       : Bridge
Neighbor Port-ID                   : mgmt
Neighbor Port-Desc                 : mgmt
TTL                                : 120
```

Showing LLDP information for the OOBM interface when there are four neighbors:

```
switch# show lldp neighbor-info mgmt

Port                               : mgmt
Neighbor Entries                   : 4
Neighbor Entries Deleted           : 0
Neighbor Entries Dropped           : 0
Neighbor Entries Aged-Out          : 0
Neighbor Chassis-Name              : switch
Neighbor Chassis-Description       : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID                : 1c:98:ec:fe:25:00
Neighbor Management-Address        : 10.1.1.2
Chassis Capabilities Available     : Bridge, Router
Chassis Capabilities Enabled       : Bridge, Router
Neighbor Port-ID                   : 1/1/1
```

```

Neighbor Port-Desc      : 1/1/1
TTL                     : 120

Neighbor Chassis-Name   : switch
Neighbor Chassis-Description : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID     : 1c:98:ec:fe:25:01
Neighbor Management-Address : 10.1.1.3
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled  : Bridge, Router
Neighbor Port-ID        : 1/1/1
Neighbor Port-Desc      : 1/1/1
TTL                     : 120

Neighbor Chassis-Name   : switch
Neighbor Chassis-Description : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID     : 1c:98:ec:fe:25:02
Neighbor Management-Address : 10.1.1.4
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled  : Bridge, Router
Neighbor Port-ID        : 1/1/1
Neighbor Port-Desc      : 1/1/1
TTL                     : 120

Neighbor Chassis-Name   : switch
Neighbor Chassis-Description : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID     : 1c:98:ec:fe:25:03
Neighbor Management-Address : 10.1.1.5
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled  : Bridge, Router
Neighbor Port-ID        : 1/1/1
Neighbor Port-Desc      : 1/1/1
TTL                     : 120

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp statistics

`show lldp statistics [<INTERFACE-ID>][vsx-peer]`

Description

Shows global LLDP statistics or statistics for a specific interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: member/slot/port .
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing global statistics for all interfaces:

```
switch# show lldp statistics
LLDP Global Statistics
=====

Total Packets Transmitted      : 19
Total Packets Received        : 19
Total Packets Received And Discarded : 0
Total TLVs Unrecognized       : 0

LLDP Port Statistics
=====
```

PORT-ID	TX-PACKETS	RX-PACKETS	RX-DISCARDED	TLVS-UNKNOWN
1/1/1	7	7	0	0
1/1/2	7	7	0	0
1/1/3	0	0	0	0
1/1/4	0	0	0	0
1/1/5	0	0	0	0
...				
mgmt	5	5	0	0
...				

Showing statistics for interface **1/1/1**:

```
switch# show lldp statistics 1/1/1

LLDP Statistics
=====

Port Name                : 1/1/1
Packets Transmitted      : 159
Packets Received         : 163
Packets Received And Discarded : 0
Packets Received And Unrecognized : 0
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp statistics mgmt

show lldp statistics mgmt

Description

Shows LLDP statistics for the OOBM interface.

Example

Showing LLDP statistics for the OOBM interface:

```
switch# show lldp statistics mgmt

LLDP Statistics
=====

Port Name                : mgmt
Packets Transmitted      : 20
Packets Received         : 23
Packets Received And Discarded : 0
Packets Received And Unrecognized : 0
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp tlv

show lldp tlv[vsx-peer]

Description

Shows the LLDP TLVs that are configured for send and receive.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show lldp tlv

TLVs Advertised
=====

Management Address
Port Description
Port VLAN-ID
System Capabilities
System Description
System Name
VLAN Name
MFS
OUI
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

aaa accounting all-mgmt

```
aaa accounting all-mgmt <CONNECTION-TYPE> start-stop {local | group <GROUP-LIST>}  
no aaa accounting all-mgmt <CONNECTION-TYPE>
```

Description

Defines accounting as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for accounting purposes.

For remote accounting, the information is sent to the first reachable remote server that was configured with this command for remote accounting. If no remote server is reachable, local accounting remains available. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote accounting.



The system accounting log is not associated with any connection type (channel) and is therefore sent to the accounting method configured on the default connection type (channel) only.

The **no** form of this command removes for the specified connection type, any defined remote AAA server group accounting sequence. Local accounting is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Defines a list of accounting server groups to be used for the default connection type. This configuration applies to all other connection types (console, https-server, ssh) that are not explicitly configured with this command. For example, if you do not use aaa accounting all-mgmt console... to define the console accounting list, then this default configuration is used for console. console Defines a list of accounting server groups to be used for the console connection type. https-server Defines a list of accounting server groups to be used for the https-server (REST, Web UI) connection type. ssh Defines a list of accounting server groups to be used for the ssh connection type.
start-stop	Selects accounting information capture at both the beginning and

Parameter	Description
	end of a process.
local	Selects local-only accounting when used without the group parameter.
group <GROUP-LIST>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server. If the AAA server(s) in the group are not reachable, or the if there is a key mismatch error between the server and the switch, the next accounting method is attempted.

Usage

Local accounting is always active. It cannot be turned off.

Examples

Setting local accounting for the default connection type:

```
switch(config)# aaa accounting all-mgmt default start-stop local
```

Setting local accounting for the console connection type:

```
switch(config)# aaa accounting all-mgmt console start-stop local
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication console-login-attempts

```
aaa authentication console-login-attempts <ATTEMPTS> console-lockout-time <LOCKOUT-TIME>
no aaa authentication console-login-attempts
```

Description

For the console interface (channel) only, enables console login attempt limiting. If the number of failed console login attempts equals the configured threshold, the user is locked out for the configured duration.

The **no** form of this command disables console login attempt limits.



Important: If you enable the lockout using this command and also enable the SSH, REST, and Telnet lockout using command **aaa authentication limit-login-attempts**, and then enter too many consecutive wrong passwords, you may become locked out, and will have to wait for the configured lockout time to elapse before logging in on any interface.



This console login attempt limiting feature is only available when not using remote authentication through AAA servers (TACACS+ or RADIUS) on any interface. Remote authentication through AAA servers (TACACS+ or RADIUS) is not possible when limit login attempts is configured on any interface.

Parameter	Description
<ATTEMPTS>	Specifies the threshold of failed console login attempts that triggers user lockout. Range: 1 to 10. For example, if <ATTEMPTS> is set to 1, a single failed login attempt triggers immediate user lockout.
<LOCKOUT-TIME>	Specifies the amount of time a user is locked out. Range: 1 to 3600 seconds.

Examples

Enabling console login attempt failure limiting with a 60 second lockout being triggered upon the third consecutive login attempt failure.

```
switch(config)# aaa authentication console-login-attempts 3 console-lockout-time 60
```

Disabling console login attempt failure limiting:

```
switch(config)# no aaa authentication console-login-attempts
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication limit-login-attempts

```
aaa authentication limit-login-attempts <ATTEMPTS> logout-time <LOCKOUT-TIME>
no aaa authentication limit-login-attempts <ATTEMPTS> logout-time <LOCKOUT-TIME>
```

Description

For the SSH, REST, and Telnet interface (channel), enables local login attempt limiting. If the number of failed local login attempts equals the configured threshold, the user is locked out for the configured duration.

The **no** form of this command disables local login attempt limits.



Important: If you enable the logout using this command and also enable the console logout using command **aaa authentication console-login-attempts**, and then enter too many consecutive wrong passwords, you may become locked out, and will have to wait for the configured logout time to elapse before logging in on any interface.



This local login attempt limiting feature is only available when not using remote authentication through AAA servers (TACACS+ or RADIUS) on any interface. Remote authentication through AAA servers (TACACS+ or RADIUS) is not possible when limit login attempts is configured on any interface.

Parameter	Description
<ATTEMPTS>	Specifies the threshold of failed local login attempts that triggers user logout. Range: 1 to 10. For example, if <ATTEMPTS> is set to 1, a single failed login attempt triggers immediate user logout.
<LOCKOUT-TIME>	Specifies the amount of time a user is locked out. Range: 1 to 3600 seconds.

Examples

Enabling local login attempt failure limiting with a 20 second logout being triggered upon the fourth consecutive login attempt failure.

```
switch(config)# aaa authentication limit-login-attempts 4 logout-time 20
```

Disabling login attempt failure limiting:

```
switch(config)# no aaa authentication limit-login-attempts
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Added Telnet support on the 10000, 9300, 83xx, 6100, 6000 and 4100i Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication login

```
aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}  
no aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}
```

Description

Defines authentication as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for authentication purposes. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote AAA authentication.

The **no** form of this command removes for the specified connection type, any defined remote AAA server group authentication sequence. Local authentication is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<code><CONNECTION-TYPE></code>	One of these connection types (channels): default Defines a list of accounting server groups to be used for the default connection type. This configuration applies to all other connection types (console, https-server, ssh) that are not explicitly configured with this command. For example, if you do not use <code>aaa accounting all-mgmt console...</code> to define the console accounting list, then this default configuration is used for console. console Defines a list of accounting server groups to be used for the console connection type. https-server Defines a list of accounting server groups to be used for the https-server (REST, Web UI) connection type. ssh Defines a list of accounting server groups to be used for the ssh connection type.

Parameter	Description
local	Selects local-only accounting when used without the group parameter.
group <GROUP-LIST>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server . If no AAA server(s) in the group are reachable, or if there is a key mismatch error between the server and the switch, the next authentication method is attempted.

Examples

Setting local authentication for the default connection type:

```
switch(config)# aaa authentication login default local
```

Setting local authentication for the console connection type:

```
switch(config)# aaa authentication login console local
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication login privilege-elevation

```
aaa authentication login privilege-elevation group administrators
no aaa authentication login privilege-elevation group administrators
```

Description

Enables/disables privilege elevation for the users in an administrators group. When enabled, an administrative user is provided lower privilege access upon successful switch login. The user must execute an `enable` command and re-authenticate to elevate their privilege to administrator (the administrator level access with '#' prompt). Executing the **disable** command revokes an administrator privilege and returns the user to the lower privilege access level (the operator level access '>' prompt). The **no** form of this command disables privilege elevation for the administrator user group.

Usage

For more information about support for local, RADIUS or TACACS+ password authentication using privilege mode, refer to the [video on the HPE Aruba Networking Airheads Broadcasting Channel](#).

Examples

Enable privilege elevation for the administrator user group:

```
switch(config)# aaa authentication login privilege-elevation group administrators
```

Disable privilege elevation for the administrator user group:

```
switch(config)# no aaa authentication login privilege-elevation group administrators
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication minimum-password-length

```
aaa authentication minimum-password-length <LENGTH>
no aaa authentication minimum-password-length <LENGTH>
```

Description

Enables minimum password length checking. Existing passwords shorter than the minimum length are unaffected. Length checking does not apply to ciphertext passwords. Length checking applies both to local and remote authentication.

The **no** form of this command disables minimum password length checking.

Parameter	Description
<LENGTH>	Specifies the minimum password length. Range: 1 to 32.

Examples

Enabling password length checking, with a minimum length of 12.

```
switch(config)# aaa authentication minimum-password-length 12
```

Disabling minimum password length checking:

```
switch(config)# no aaa authentication minimum-password-length
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authorization commands (local)

```
aaa authorization commands <CONNECTION-TYPE> {local | none}  
no aaa authorization commands <CONNECTION-TYPE> {local | none}  
aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>  
no aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
```

Description

Defines authorization as being basic local RBAC (specified as **none**), or as full-fledged local RBAC specified as **local** (the default), or as remote TACACS+ (specified with `group <GROUP-LIST>`). Each available connection type (channel) can be configured individually. All server groups named in the command, must exist. This command can be issued multiple times, once for each connection type.

The **no** form of this command unconfigures authorization for the specified connection type, reverting to the default of **local**.



Although only TACACS+ servers are supported for remote authorization, local authorization (basic or full-fledged) can be used with remote RADIUS authentication. If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Parameter	Description
<code><CONNECTION-TYPE></code>	One of these connection types (channels): <code>default</code> Selects the default connection type for configuration. This configuration applies to all other connection types (console, ssh) that are not explicitly configured with this command. For example, if you do not use aaa authorization commands console... to define the console authorization list, then this default configuration is used for console. <code>console</code> Selects the console connection type for configuration. <code>ssh</code> Selects the ssh connection type for configuration.
<code>local</code>	When used alone without <code>group <GROUP-LIST></code>, selects local authorization which can be used to provide authorization for a purely local setup without any remote AAA servers and also for when RADIUS is used for remote Authentication and Accounting but Authorization is local. When used after <code>group</code>, provides for fallback (to full-fledged local authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: If any TACACS+ server in the specified groups is reachable, but the command fails to be authorized by that server, the command is rejected and local authorization is never attempted. Local authorization is only attempted if every TACACS+ server cannot be reached.
<code>none</code>	When used alone without <code>group <GROUP-LIST></code>, selects basic local RBAC authorization, for use with the built-in user groups (administrators, operators, auditors). When used after <code>group</code>, provides for fallback (to basic local RBAC authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: With none, for users belonging to user-defined user groups, all commands can be executed regardless of what authorization rules are defined in such groups. For per-command local authorization, use local instead.
<code>group <GROUP-LIST></code>	Specifies the list of remote AAA server group names. Predefined remote AAA group name tacacs is available. User-defined TACACS+ server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa server group and servers are added to a server group using command server. It is recommended to always include either the special name local or none as the last name in the group list. If both local or none are omitted, and no remote AAA server is reachable (or the first reachable server cannot authorize the command), command execution for the current user will not be possible. If no AAA server(s) in the group are reachable, or if there is a key mismatch error between the server and the switch, the next authorization method is attempted.

Examples

Setting the authorization for default to **local**:

```
switch(config)# aaa authorization commands default local
```

Setting the authorization for the SSH interface to **none**:

```
switch(config)# aaa authorization commands ssh none
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show aaa accounting

```
show aaa accounting [vsx-peer]
```

Description

Shows the accounting configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing local accounting for the default and console connection types:

```
switch(config)# aaa accounting all default start-stop local
switch(config)# aaa accounting all console start-stop local
switch(config)# exit
switch# show aaa accounting
AAA Accounting:
  Accounting Type           : all
  Accounting Mode           : start-stop

Accounting for default channel:
```

```

-----
GROUP NAME | GROUP PRIORITY
-----
local | 0
-----

Accounting for console channel:
-----
GROUP NAME | GROUP PRIORITY
-----
local | 0
-----

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication

show aaa authentication [vsx-peer]

Description

Shows the authentication configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing local authentication for the default and console connection types (channels):

```

switch(config)# aaa authentication login default local
switch(config)# aaa authentication login console local
switch(config)# exit

```

```
switch# show aaa authentication

AAA Authentication:
  Fail-through           : Disabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set
```

Authentication for default channel:

```
-----
GROUP NAME | GROUP PRIORITY
-----
local      | 0
-----
```

Authentication for console channel:

```
-----
GROUP NAME | GROUP PRIORITY
-----
local      | 0
-----
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authorization

```
show aaa authorization [vsx-peer]
```

Description

Shows the authorization configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing full-fledged local RBAC authorization for the default and console connection types (channels):

```
switch(config)# aaa authorization commands default none
switch(config)#
switch(config)# aaa authorization commands console none
switch(config)# exit
switch#
switch# show aaa authorization
Authorization for default channel:
```

GROUP NAME	GROUP PRIORITY
none	0

Authorization for console channel:

GROUP NAME	GROUP PRIORITY
none	0



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show authentication locked-out-users

show authentication locked-out-users

Description

Shows a list of users currently locked out due to excessive failed login attempts. This applies to console, REST, SSH, WebUI, and telnet logins.

Example

Showing locked-out users.

```
switch# show authentication locked-out-users
USER                                GROUP
```



```
-----  
admin                administrators  
admin-1             administrators
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	The output of this command now also includes information for users locked out due to excessive REST login attempts.
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ssh authentication-method

```
show ssh authentication-method
```

Description

Shows the status of the SSH public key method and the local password-based (through SSH client) authentication method.

Example

Showing the authentication methods.

```
switch# show ssh authentication-method  
SSH publickey authentication : Enabled  
SSH password authentication : Enabled
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show user

`show user <USERNAME> authorized-key`

Description

Shows the SSH client public key list for a specified user.

Parameter	Description
<code><USERNAME></code>	Specifies the username for which you want to show the SSH client public key list.

Usage

Any user can show their own public key list; however, administrators can also show a public key list of other users.

Examples

Showing a client public key:

```
switch# show user admin authorized-key

1. Key Type : RSA      Key size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDMtyMBmmAaF6r1zxf3DZNHSYVHBjhlbBlyAIqQ8DSHK
...
U+aE14UW/ifiukmK67sIHwK+FhhRYwPztQc5pjyOPk128a4pgKQaHCcOF169Z admin@switch
```

Showing two client public keys:

```
switch# show user admin authorized-key

1. Key Type : ECDSA      Curve : nistp256
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEgEFevZ0
...
176V+D0svdCJ9Wo32zqI9OeAdTJw/eZYp5qknhNgS81HjAI6J/4/kAqdZAJbqQUiCAk= admin@switch

2. Key Type : RSA      Key size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDXQHrqV7+/GcMdOhr//IRjJkX7TQKupW89j80bL7xq8
...
j8qKuHWSN0/h/HxjzQJuYDVmZN5vG3DhpXbBZU1ZNnchVod13QLCesqA3VLKN admin@switch
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ssh password-authentication

`ssh password-authentication`

`no ssh password-authentication`

Description

Enables the password-based authentication method for use with SSH clients.

The **no** form of this command disables the password-based authentication method for use with SSH clients.

Usage

The switch ships with password-based authentication (for SSH clients) enabled. The maximum number of password retries is three.

Examples

Enabling password authentication for use with SSH clients:

```
switch(config)# ssh password-authentication
```

Disabling password authentication for use with SSH clients:

```
switch(config)# no ssh password-authentication
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh public-key-authentication

```
ssh public-key-authentication
no ssh public-key-authentication
```

Description

Enables the SSH public key authentication method. The switch ships with SSH public key authentication enabled.

The **no** form of this command disables the SSH public key authentication method.



Although SSH public key authentication is enabled by default, it cannot be used until SSH public keys are added with the **user authorized-key** command.

Examples

Enabling SSH public key authentication:

```
switch(config) # ssh public-key-authentication
```

Disabling SSH public key authentication:

```
switch(config) # no ssh public-key-authentication
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

user authorized-key

```
user <USERNAME> authorized-key <PUBKEY>
no user <USERNAME> authorized-key [<KEYNUM>]
```

Description

Copies an SSH client public key into the key list. If the key list and the public key do not exist, it creates a list with the public key. If the SSH client public key exists, the command appends the new key to the existing list. The client public key list holds a maximum of 32 client keys.

The **no** form of the command removes either one or all SSH public keys from the key list.

Parameter	Description
<code><USERNAME></code>	Specifies the name of the user.
<code><PUBKEY></code>	Specifies the SSH client public key to be copied into the key list.
<code><KEYNUM></code>	Specifies the key number. The range is 1 to 32. Use the show user <USERNAME> authorized-key command to find the key number associated with the key.

Usage

Each key on the key list has a key identifier. The **show user <USERNAME> authorized-key** command displays the key identifier associated with the key.

Administrators can add and remove the public keys of themselves and other users. Operators can add and remove only their own public keys. If the public key authentication method is enabled, the client public key present is used by the SSH server to authenticate the client. The authentication method reverts to the password authentication method and prompts for a client password when one of the following occurs:

- The client public keys are not present.
- The server does not have the keys enabled.
- The public key method is disabled.

You can either remove all keys or a specific key. Each key on the key list has a key identifier. If you provide the key identifier in this command, the command removes the corresponding key from the list. If you provide no key identifier, the command removes all keys from the key list.

Examples

Adding a public key:

```
switch(config)#user admin authorized-key ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBEqEFevZ0176V+D0svdCJ9Wo32zqI9OeAIdTJwT/eZYp50qkA  
nhZNgs81HBjAI6QJ/4/kAyqdZ9oAjbicQUiCAk= root@switch
```

Removing all SSH public keys from the list:

```
switch(config)# no user admin authorized-key
```

Removing the specified SSH public key from the list:

```
switch(config)# no user admin authorized-key 2
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

logging threshold

```
logging threshold {audit-log | auth-log | commands-log | event-log | | https-server-log}
<THRESHOLD%>
no logging threshold {audit-log | auth-log | commands-log | event-log | | https-server-
log} [<THRESHOLD%>]
```

Description

Selects the logging buffer notification threshold for the specified logging buffer. Whenever the logging buffer space consumption exceeds the selected threshold (percent of buffer capacity), a LOG_BUFFER_ALMOST_FULL event and SNMP RMON trap is triggered. This gives you the opportunity to save the logs elsewhere before the buffers are rotated with the oldest data being overwritten.

Also, a LOG_BUFFER_WRAPPED event and SNMP RMON trap is triggered if the logging buffer capacity is fully consumed and the log buffer is rotated with the oldest data being overwritten.

The **no** form of this command resets the logging buffer warning threshold to its default. All logs except **audit-log** have a default of 90 (percent) and **audit-log** has a default of 50 (percent).



The largest REST payload that can be sent to RADIUS/TACACS servers is 1024 characters, and the maximum REST payload that can be sent to syslog servers is 3500 characters. Once this limit is exceeded, the log will display three dots (...) to indicate the the message has exceeded the character limit and is incomplete. .

Parameter	Description
audit-log	Selects the audit log.
auth-log	Selects the authentication log.
commands-log	Configure the logging threshold for commands log buffer
event-log	Selects the event log.
https-server-log	Selects the HTTPS server log.
<THRESHOLD%>	Selects the notification threshold as a percent that the selected logging buffer is full. Available percent values for all logs except audit-log: 15 30 50 70 90 100 Available percent values for audit-log: 50 100

Examples

Setting the audit log threshold:

```
switch(config)# logging threshold audit-log 100
```

Setting the authentication log threshold:

```
switch(config)# logging threshold auth-log 50
```

Setting the event log threshold:

```
switch(config)# logging threshold event-log 70
```

Setting the HTTPS server log threshold:

```
switch(config)# logging threshold https-server-log 50
```

Resetting the audit log threshold to its default of 50:

```
switch(config)# no logging threshold audit-log
```

Resetting the authentication log threshold to its default of 90:

```
switch(config)# no logging threshold auth-log
```

Resetting the event log threshold to its default of 90:

```
switch(config)# no logging threshold event-log
```

Resetting the HTTPS server log threshold to its default of 90:

```
switch(config)# no logging threshold https-server-log
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.11	Introduced the commands-log parameter.
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

logrotate maxsize

logrotate maxsize <MAX-SIZE>
no logrotate maxsize

Description

Specifies the maximum allowed log file size.

A log file that exceeds either the **logrotate maxsize** or the **logrotate period** (whichever happens first), triggers rotation of the log file.

The **no** form of this command resets the size of the log file to the default (100 MB).

Parameter	Description
<MAX-SIZE>	Specifies the allowed size the log file can reach before it is compressed and stored locally or transferred to a remote host. Range: 10 to 200 MB. Default: 100 MB.

Examples

Setting the maximum log file size:

```
switch(config)# logrotate maxsize 24
```

Resetting the maximum log file size to its default of 100 MB:

```
switch(config)# no logrotate maxsize
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

logrotate period

logrotate period {daily | hourly | monthly | weekly}
no logrotate period

Description

Sets the log file rotation time period. Defaults to daily.

A log file that exceeds either the **logrotate maxsize** or the **logrotate period** (whichever happens first), triggers rotation of the log file.

The **no** form of this command resets the log rotation period to the default of daily.

Parameter	Description
daily	Rotates log files on a daily basis (default) at 0:01.
hourly	Rotates log files every hour at the first second of the hour.
monthly	Rotates log files monthly on the first day of the month at 00:01.
weekly	Rotates log files once a week on Sunday at 00:01.

Examples

Setting a weekly period:

```
switch(config)# logrotate period weekly
```

Resetting the period to its default of daily:

```
switch(config)# no logrotate period
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

logrotate target

```
logrotate target <URI> [vrf <VRF_NAME>]  
no logrotate target [<URI>] [vrf <VRF_NAME>]
```

Description

Using TFTP, sends the rotated log files to a specified remote host identified by Universal Resource Identifier (URI).

The **no** form of this command resets the target to the default, which stores the rotated and compressed log files locally in **/var/log/**.

Command context

Parameter	Description
<URI>	Specifies the URI of the remote host. The default directory is local. tftp://{<IPV4_ADDR> IPV6_ADDR}<HOST> [/<DIRECTORY>]
<VRF_NAME>	Specifies the VRF name (Default: default).

Usage

- Rotated log files are compressed and stored locally in the path **/var/log/** regardless of the remote host configuration.

Examples

Setting an IPv4 target:

```
switch(config)# logrotate target tftp://192.168.1.132
```

Setting an IPv4 target with a directory:

```
switch(config)# logrotate target tftp://192.168.1.132/logrotate/
```

Setting an IPv4 target with the default VRF:

```
switch(config)# logrotate target tftp://192.168.1.132 vrf mgmt
```

Setting an IPv6 target with the default VRF:

```
switch(config)# logrotate target tftp://2001:db8:0:1::128 vrf default
```

Resetting the target to local:

```
switch(config)# no logrotate target
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.09	Updated the syntax and examples.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show logrotate

show logrotate [vsx-peer]

Description

Shows the log rotate configuration.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show logrotate
Logrotate configurations :
Period           : weekly
Maxsize          : 20MB
Target           : tftp://2001:db8:0:1::128 vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

loop-protect

```
loop-protect
no loop-protect
```

Description

Enables loop protection on a layer 2 interface, VXLAN interface, or LAG. Loop protection packets are sent/received on the LAG and not the interface which are members of the LAG. Loop protection only works on layer 2 interfaces. If a layer 2 interface is changed to a layer 3 interface, all loop protection configuration settings are lost for that interface.

If loop protection is enabled on a VXLAN interface, the local VTEP will generate loop protect packets on the VXLAN tunnel. Remote VTEP will hardware forward the same loop protect packet. If a local VTEP receives its own packet on any L2 interface, it will be detected as a loop and will bring down the L2 interface on which the loop protect control packet was received.

The **no** form of this command disables loop protection on a layer 2 interface, VXLAN interface, or LAG.



Loop protection on VXLAN interfaces is supported only on AOS-CX 6200,6300,6400,8360,8325,8400,9300,8100,10000 switch series.

Examples

Enabling loop protection on interface **1/1/1**:

```
switch# config
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# loop-protect
```

Enabling loop protection on LAG **25**:

```
switch# config
switch(config)# interface lag 25
switch(config-if)# no routing
switch(config-lag-if)# loop-protect
```

Enabling loop protection on VXLAN interface:

```
switch# config
switch(config)# interface vxlan 1
switch(config-vxlan-if)# loop-protect
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.12	Loop protection supported on VXLAN interfaces.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-lag-if config-vxlan-if	Administrators or local user group members with execution rights for this command.

loop-protect action

```
loop-protect action {do-not-disable | tx-disable | tx-rx-disable}  
no loop-protect action {do-not-disable | tx-disable | tx-rx-disable}
```

Description

Sets the action to be taken when a loop protection packet is received on a port.

If an action is configured after a loop is detected, then the new action only takes effect after the re-enable timer expires. To have the action take effect immediately, disable and then re-enable loop protect.

The **no** form of this command resets the action to the default (**tx-disable**).



This command is not supported on a VXLAN interface and the default action for a VXLAN interface is rx-disable .

Parameter	Description
do-not-disable	No ports are disabled. On every transmit interval, the loop will be detected and the detection will be reported via an SNMP trap and an event log message.
tx-disable	The port that transmitted the loop detection packet is disabled. When this setting is enabled, environments with N loops, must have loop protection be configured on at least N-1 ports to have a loop free topology. Default.
tx-rx-disable	The ports that transmitted and received the loop detection packet are disabled.

Example

```
switch(config-if)# loop-protect action do-not-disable
switch(config-if)# no loop-protect action do-not-disable
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

loop-protect re-enable-timer

```
loop-protect re-enable-timer <TIME>
no loop-protect re-enable-timer <TIME>
```

Description

Configures the time interval after which an interface disabled by loop protection is re-enabled. The loop protection timer is disabled by default.

The **no** form of this command disables the loop protect timer.

Parameter	Description
<TIME>	Specify the number of seconds after which a disabled interface is re-enabled. Range: 15 to 604800.

Example

```
switch# config
switch(config)# loop-protect re-enable-timer 60
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

loop-protect transmit-interval

```
loop-protect transmit-interval <TIME>
no loop-protect transmit-interval [<TIME>]
```

Description

Configures the time interval between successive loop protect packets sent on an interface. The **no** form of this command sets the time interval to the default value of 5 seconds.

Parameter	Description
<TIME>	Configures the transmit interval in seconds. Range: 5 to 10. Default: 5.

Examples

```
switch(config)# loop-protect transmit-interval 10
switch(config)# no loop-protect transmit-interval
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

loop-protect trap loop-detected

```
loop-protect trap loop-detected
no loop-protect trap loop-detected
```

Description

Enables sending SNMP traps for loop-protect related events.

The **no** form of this command disables sending SNMP traps for loop-protect related events.

Examples

Enabling the sending of SNMP traps:

```
switch# loop-protect trap loop-detected
```

Disabling the sending of SNMP traps:

```
switch# no loop-protect trap loop-detected
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

loop-protect vlan

```
loop-protect vlan <VLAN-LIST>  
no loop-protect vlan
```

Description

Specifies the trunk allowed VLANs on which loop protection packets are sent. By default, loop protection packets are only sent on access VLANs and native VLANs on a port. To send loop protection packets on trunk allowed VLANs, the VLANs must be explicitly added using this command.

When loop protection is enabled on VXLAN interfaces, the switch will start transmitting loop protect packets to each VTEP peer that are part of a VNI.

Loop protection can be configured on a maximum of 4094 VLANs across all interfaces.

Loop protection on VXLAN interfaces can be enabled on a maximum of 5000 (total of number of VTEPs * number of loop protect enabled VLANs). Loop protection will generate a maximum 5000 VXLAN encapsulated packets within the default loop protect time interval of 5 seconds.

The **no** form of this command removes loop protection from all VLANs on the interface.

Parameter	Description
<VLAN-LIST>	Specifies the number of a single VLAN, or a series of numbers for a range of VLANs, separated by commas (1, 2, 3, 4), dashes (1-4), or both (1-4, 6).

Example

```
switch(config-if) # loop-protect vlan 2-6,10,15-20
```

Enabling loop protection on VXLAN interface:

```
switch# config
switch(config) # interface vxlan 1
switch(config-lag-if) # loop-protect vlan 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.12	Loop protection supported on VXLAN interfaces.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if config-vxlan-if	Administrators or local user group members with execution rights for this command.

show loop-protect

Description

```
show loop-protect [<INTERFACE-NAME>] [vsx-peer]
```

This command shows the following global configurations.

- Transmit interval.
- Re-enable timer.
- Per-port configurations.
- Loop-protect enable or disable status.
- Loop detection.
- Loop detected count.
- Timestamp of latest loop detection.

- Loop is detected on VLAN.
- Interface status.
- List of configured VLAN's for that port.
- VTEP port information

Specify the interface name on display for the filter. When rebooting the switch or after switchover, The loop-detected count on the loop detected port is reset to zero.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the name of a logical interface on the switch. This can be one of the following: ▪ An Ethernet interface associated with a physical port. Format: member/slot/port. ▪ A LAG (link aggregation group). Specify the ID of LAG . For example: lag100. ▪ A VXLAN interface. Specify the VXLAN ID. For example: vxlan 1.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.



Loop protection on VXLAN interfaces is supported on HPE Aruba Networking 5420, 6200, 6300, 6400, 8360, 8325, 8400, 9300/9300S, 8100, 10000 switch series.

Examples

```
switch# show loop-protect

Transmit Interval (sec)           : 5
Port Re-enable Timer (sec)       : Disabled
Loop Detected Trap                : Enabled

Interface 1/1/1
  Loop-protect enabled           : Yes
  Loop-Protect enabled VLANs     :
  Action on loop detection       : TX disable
  Loop detected count            : 0
  Loop detected                  : No
  Interface status               : up

Interface 1/1/2
  Loop-protect enabled           : Yes
  Loop-Protect enabled VLANs     :
  Action on loop detection       : TX disable
  Loop detected count            : 0
  Loop detected                  : No
  Interface status               : up

Interface vxlan 1
  Loop-protect enabled           : Yes
  Loop-Protect enabled VLANs     :
  Action on loop detection       : RX disable
  Loop detected count            : 0
  Loop detected                  : No
```

```
Interface status          : up
```

```
switch# show loop-protect 1/1/3
```

Status and Counters - Loop Protection Information

```
Transmit Interval (sec)      : 5
Port Re-enable Timer (sec)   : 0
Loop Detected Trap           : Disabled
```

Interface 1

```
Loop-protect enabled         : Yes
Loop-Protect enabled VLANs   :
Action on loop detection     : TX disable
Loop detected count          : 0
Loop detected                 : No
Interface status              : up
```

```
switch# show loop-protect
```

Status and Counters - Loop Protection Information

```
Transmit Interval           : 5 (sec)
Port Re-enable Timer        : Disabled
Loop Detected Trap          : Disabled
```

Interface 1/5/48

```
Loop-protect enabled        : No
Action on loop detection     : TX disable
Loop detected count          : 1
Loop detected                 : Yes
Detected on VLAN             : 100
Detected at                  : 2023-03-20T00:01:17
Interface status             : down
Tx_port                       : VTEP_100.1.1.2
```

Interface vxlan1

```
Loop-protect enabled        : Yes
Loop-Protect enabled VLANs   : 100
Action on loop detection     : RX disable
Loop detected count          : 0
Loop detected                 : No
Interface status             : up
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.12	Loop protection supported on VXLAN interfaces.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

interface loopback

```
interface loopback <INSTANCE>
no interface loopback <INSTANCE>
```

Description

Creates a loopback interface and enters loopback configuration mode.
The **no** form of this command deletes a loopback interface.

Parameter	Description
<INSTANCE>	Selects the loopback interface ID. Range: 0 to 255

Examples

```
switch(config)# interface loopback
switch(config-loopback-if)#
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip address

```
ip address <IPv4-ADDR/MASK> [secondary]
no ip address <IPv4-ADDR/MASK> [secondary]
```

Description

Sets the IPv4 address for a loopback interface.

The **no** form of this command reverses the set of the IPv4 address for a loopback interface.

Parameter	Description
<i><IPv4-ADDR></i>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<i><MASK></i>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<i>secondary</i>	Indicates that the IPv4 address is a secondary address.

Examples

```
switch(config)# interface loopback 1
switch(config-loopback-if)# ip address 16.93.50.2/24
switch(config-loopback-if)# ip address 20.1.1.1/24 secondary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 address

ipv6 address *<IPv6-ADDR/MASK>*

Description

Sets the IPv6 address for a loopback interface.

Parameter	Description
<i><IPv6-ADDR></i>	Specifies an IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<i><MASK></i>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

```
switch(config)# interface loopback 1  
switch(config-loopback-if)# ipv6 address fd00:5708::f02d:4df6/64
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

vrf attach

```
vrf attach <VRF-NAME>  
no vrf attach <VRF-NAME>
```

Description

Attaches a non-default VRF to a loopback.

The **no** form of this command deletes a non-default VRF from a loopback and reattaches the default VRF.

Parameter	Description
<VRF-NAME>	Specifies the name of the non-default VRF to be attached/deleted to/from a loopback.

Examples

```
switch(config)# interface loopback 1  
switch(config-loopback-if)#vrf attach test
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface loopback

show interface loopback [brief | instance <ID>] [vsx-peer]

Description

This command displays the configuration and status of loopback interfaces.

Parameter	Description
brief	Displays brief information about all configured loopback interfaces.
instance <ID>	Displays the configuration and status of a loopback interface ID. Range: 1-255
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show interface loopback
Interface loopback1 is up
IPv4 address 192.168.1.1/24
Interface loopback2 is up
IPv4 address 182.168.1.1/24
```

```
switch# show interface loopback brief
-----
Loopback      IP Address                      Status
Interface
-----
loopback1    10.1.1.1/24                     up
loopback1    1111:2222:3333:4444::6666/128  up
```

```
switch# show interface loopback 1
Interface loopback1 is up
IPv4 address 192.168.1.1/24
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear mac-address

```
clear mac-address {interface <INTERFACE> | port <PORT-NUM> [vlan <VLAN-ID>] | vlan <VLAN-ID> [port <PORT-NUM>] | <MAC-ADDR> [vlan <VLAN-ID>] [force] | <mac-address mac-move [address <mac-address> vlan <vlan>] | [vlan <VLAN>] <VLAN-ID>]}
```

Description

Clears the dynamic learned MAC addresses on the specified interface, combination of interface and VLAN, port, VLAN, combination of port and VLAN, MAC address, or combination of MAC address and VLAN. The command does not clear any port-security learned MAC addresses.

Port-security MAC addresses are cleared when the port on which the MAC addresses were learned are shut down or the port-access-security feature is disabled on the port or the switch.

Parameter	Description
<INTERFACE>	Specifies the list of interfaces, for example, 1/1/1 or 1/1/1-1/1/3 or lag1 or vlan1 .
<PORT-NUM>	Specifies a physical port on the switch. Format: member/slot/port .
<VLAN-ID>	Specifies the number of a VLAN.
<MAC-ADDR>	Specifies the MAC address.
<mac-address mac-move>	Clears the MAC move count and move history for a specified list or range of VLANs, or for a specific MAC address and VLANs. When the MAC address and VLANs are not mentioned, the statistics for all MAC addresses are cleared.
force	Clears the specified MAC address even if the MAC address is internally programmed by MAC management.

Examples

Clearing the learned MAC addresses on a port:

```
switch# clear mac-address port 1/1/1
```

Clearing the learned MAC addresses on a combination of a VLAN and a port:

```
switch# clear mac-address port 1/1/1 vlan 20
```

```
switch# clear mac-address vlan 2 port 1/1/3
```

Clearing the learned MAC addresses on a combination of a VLAN and an interface or a list of interfaces:

```
switch# clear mac-address interface 1/1/1 vlan 10
```

```
switch# clear mac-address vlan 1 interface 1/1/1-1/1/3
```

Clearing the specified MAC addresses entry on the VLAN:

```
switch# clear mac-address 14:FA:01:F1:8B:8F vlan 1
```

Clearing the specified MAC addresses entry by force:

```
switch# clear mac-address 14:FA:01:F1:8B:8F force
```

Clearing the learned MAC move addresses on a port:

```
switch# clear mac-address mac-move
```

Clearing the learned MAC move addresses on a combination of a VLAN and an interface or a list of interfaces:

```
switch# clear mac-address mac-move address 00:00:00:00:00:01 vlan 10
```

Clearing the MAC move addresses entries on the VLAN:

```
switch# clear mac-address mac-move vlan 10-20
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.13	The mac-address mac-move parameter was introduced.
10.09	Added parameters for interface and MAC address.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

clear mac address mac move

```
clear mac-address mac-move [address <mac-address> vlan <vlan>] | [vlan <VLAN>]
```

Description

Clears the MAC move count and move history for a specified list or range of VLANs, or for a specific MAC and VLAN.

When MAC and VLAN are not mentioned, it clears statistics for all MACs.

Parameter	Description
<address>	Clears information for a specific MAC address.
<vlan>	Clears mac-move entries on VLANs.

Examples

Clearing the learned MAC move addresses on a port:

```
switch# clear mac-address mac-move
```

Clearing the learned MAC move addresses on a combination of a VLAN and an interface or a list of interfaces:

```
switch# clear mac-address mac-move address 00:00:00:00:00:01 vlan 10
```

Clearing the MAC move addresses entries on the VLAN:

```
switch# clear mac-address mac-move vlan 10-20
```

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

clear mac-address-table

```
clear mac-address-table
  address <mac-address>
  vlan <1-4094>
```

Description

This command is used to clear the MAC move count and move history for a single MAC address or VLAN, or for a range of VLANs. If no specific MAC address or VLAN is specified, this command clears statistics for all MAC addresses.

Parameter	Description
address	(Optional) Clear information for a specific MAC address.
vlan <1-4094>	(Optional) Clear move information for specific VLAN.

Examples

Clearing MAC move statistics for all MAC addresses.

```
switch# clear mac-address mac-move
```

Clearing MAC move statistics for MAC addresses in a range of VLANs.

```
switch# clear mac-address mac-move vlan 10-20
```

Clearing MAC move addresses from a specific MAC address and VLAN:

```
switch# clear mac-address mac-move address 00:00:00:00:00:01 vlan 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.13 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

mac-address-table age-time

```
mac-address-table age-time <SECONDS>
no mac-address-table age-time [<SECONDS>]
```

Description

Sets the maximum amount of time a MAC address remains in the MAC address table. When this time expires, the MAC address is removed.

The **no** form of this command resets the MAC aging timer to the default value (300 seconds).

Parameter	Description
age-time <SECONDS>	Specifies the MAC address aging time in seconds. Range: 60 to 3600. Default: 300.

Example

```
switch(config)# mac-address-table age-time 120
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show mac-address-table

```
show mac-address-table [hsc] [vsx-peer]
```

Description

Shows MAC address table information. If HSC is enabled, MAC addresses discovered by the HSC manager are also displayed.

Parameter	Description
[hsc]	Displays only MAC address discovered by the HSC manager on the remote controller.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing output when table entries exist:

```
switch# show mac-address-table
MAC age-time           : 300 seconds
Number of MAC addresses : 5
```

MAC Address	VLAN	Type	Port
00:00:00:00:00:05	1	dynamic	1/1/2
00:00:00:00:00:06	2	dynamic	1/1/1
00:00:00:00:00:08	3	hsc	vxlan1(10.1.1.1)
00:00:00:00:00:12	3	hsc	vxlan1(10.1.1.3)
00:00:00:00:00:34	3	hsc	vxlan1(10.1.1.4)

Showing output that includes information about an IPv6 VXLAN:

```
3C-T-6300-27# show mac-address-table
MAC age-time           : 300 seconds
Number of MAC addresses : 2
```

MAC Address	VLAN	Type	Port
00:50:56:8d:44:13	1001	dynamic	1/1/2
00:50:56:8d:45:63	1002	evpn	vxlan1(1920:1680:1:1::2)

Showing output when there are no MAC table entries:

```
switch# show mac-address-table
No MAC entries found.
```

Showing only MAC address discovered by the HSC manager:

```
switch# show mac-address-table hsc
Number of MAC addresses : 3
```

MAC Address	VLAN	Type	Port
00:00:00:00:00:08	3	hsc	vxlan1(10.1.1.1)
00:00:00:00:00:12	3	hsc	vxlan1(10.1.1.3)
00:00:00:00:00:34	3	hsc	vxlan1(10.1.1.4)



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table address

`show mac-address-table address <MAC-ADDR> [vsx-peer]`

Description

Shows MAC address table information for a specific MAC address.

Parameter	Description
<MAC-ADDR>	Specifies the MAC address.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show mac-address-table address 00:00:00:00:00:01
MAC age-time           : 300 seconds
Number of MAC addresses : 2

MAC Address      VLAN    Type      Port
-----
00:00:00:00:00:01  2      dynamic   1/1/1
00:00:00:00:00:01  1      dynamic   1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table count

```
show mac-address-table count
[dynamic | port <PORT-NUM> | vlan <VLAN-ID>] [vsx-peer]
```

Description

Displays the number of MAC addresses.

Parameter	Description
dynamic	Show the count of dynamically learned MAC addresses.
<PORT-NUM>	Specifies a physical port on the switch. Format: member/slot/port .
vlan <VLAN-ID>	Specifies the number of a VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the number of MAC addresses:

```
switch# show mac-address-table count
Number of MAC addresses : 8
```

Showing the number of dynamically learned MAC addresses:

```
switch# show mac-address-table count dynamic
Number of MAC addresses : 8
```

Showing the number of MAC addresses per physical port on the switch:

```
switch# show mac-address-table count port 1/1/1
Number of MAC addresses : 2
```

Showing the number of MAC addresses per VLAN:

```
switch# show mac-address-table count vlan 100
Number of MAC addresses : 5
```

Showing the number of MAC addresses on the VSX primary and secondary (peer) switch:

```
vsx-primary# show mac-address-table count
Number of MAC addresses : 26114
vsx-primary# show mac-address-table count vsx-peer
Number of MAC addresses : 26113
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table dynamic

```
show mac-address-table dynamic [port <PORT-NUM> | vlan <VLAN-ID>] [vsx-peer]
```

Description

Shows MAC address table information about dynamically learned MAC addresses.

Parameter	Description
<PORT-NUM>	Specifies a physical port on the switch. Format: member/slot/port .
<VLAN-ID>	Specifies the number of a VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing all dynamic MAC address table entries:

```
switch# show mac-address-table dynamic
MAC age-time          : 300 seconds
Number of MAC addresses : 2
```

MAC Address	VLAN	Type	Port
00:00:00:00:00:05	1	dynamic	1/1/2
00:00:00:00:00:06	2	dynamic	1/1/1

Showing dynamic MAC address table entries for VLAN 1:

```
switch# show mac-address-table dynamic vlan 1
MAC age-time           : 300 seconds
Number of MAC addresses : 1

MAC Address      VLAN    Type      Port
-----
00:00:00:00:00:05  1      dynamic   1/1/2
```

Showing dynamic MAC address table entries for port **1/1/1**:

```
switch# show mac-address-table dynamic port 1/1/1
MAC age-time           : 300 seconds
Number of MAC addresses : 1

MAC Address      VLAN    Type      Port
-----
00:00:00:00:00:06  2      dynamic   1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table interface

```
show mac-address-table interface <INTERFACE>
```

Description

Shows the MAC address table entries for the specified interface.

Parameter	Description
<INTERFACE>	Specifies an interface or a list of interfaces on the switch.

Examples

Showing the MAC address table entries for interface **1/1/1**:

```
switch# show mac-address-table interface 1/1/1
MAC age-time           : 300 seconds
Number of MAC addresses : 1

MAC Address      VLAN    Type      Interface
-----
00:00:00:00:00:01  2      dynamic   1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table lockout

```
show mac-address-table lockout [vsx-peer]
```

Description

Shows MAC lockout table information.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show mac-address-table lockout
Number of MAC lockout addresses :

2MAC Address      Type
-----
00:00:00:00:01:10  static
00:00:00:00:10:03  static
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac address table mac move

```
show mac-address-table mac-move [address <mac-address> vlan <vlan>] | [vlan <vlan>]
```

Description

Displays the MAC entries in the MAC address table that have moved at least once.

The output can be filtered based on a specific VLAN or specific MAC address and VLAN.

Parameter	Description
<address>	Displays information for a specific MAC address.
<vlan>	Displays information for specific VLANs.

Examples

Displaying the moved MAC addresses:

```
switch# show mac-address-table mac-move
Number of MAC addresses : 2

MAC Address      VLAN    Current Port    Previous Port    Move Count    Last Move
-----
00:00:00:00:00:bb 10      1/1/28          1/1/27          2             Fri Sep 15
19:11:52 2023
00:00:00:00:00:aa 10      1/1/27          1/1/28          2             Fri Sep 15
19:11:51 2023

switch# show mac-address-table mac-move address 00:00:00:00:00:aa vlan 10
Number of MAC Move addresses : 1

MAC Address      VLAN    Current Port    Previous Port    Move Count    Last Move
```

```

-----
00:00:00:00:00:aa 10      1/1/27      1/1/28      2      Fri Sep 15
19:11:51 2023

switch# show mac-address-table mac-move vlan 10
Number of MAC Move addresses : 2

MAC Address          VLAN    Current Port    Previous Port    Move Count    Last Move
-----
00:00:00:00:00:bb 10      1/1/28      1/1/27      2      Fri Sep 15
19:11:52 2023
00:00:00:00:00:aa 10      1/1/27      1/1/28      2      Fri Sep 15
19:11:51 2023

```



In the case of MACs learned on VXLAN tunnels or "port-access port-security" enabled ports, the move scenario is handled by the EVPN/port-access feature respectively and it performs the move by deleting the MAC from the old port and installing it on new port. Thus, the MAC move data will be removed for the deleted MAC addresses.

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show mac-address-table mac-move

```

show mac-address-table mac-move
  address <mac-address>
  vlan <1-4094>

```

Description

This command displays the MAC entries in the MAC address table that have moved at least one time. The output of this command can be filtered to display information for a specific VLAN or for a specific MAC address and VLAN.



Users will not be able to view mac-move count for clients that are transitioning between mac-auth enabled ports; however, users will be able to view the mac-move count when clients are transitioning from a mac-auth enabled port to a non-authenticated port.

Parameter	Description
address	(Optional) Show move information for a specific MAC address.
vlan <1-4094>	(Optional) Show move information for specific VLAN.

Examples

Showing the total number of MAC move addresses:

```
switch# show mac-address-table mac-move
Number of MAC Move addresses : 2
```

MAC Address	VLAN	Current Port	Previous Port	Move Count	Last Move
00:00:00:00:00:bb 19:11:52 2023	10	1/1/28	1/1/27	2	Fri Sep 15
00:00:00:00:00:aa 19:11:51 2023	10	1/1/27	1/1/28	2	Fri Sep 15

Showing the number MAC move addresses on a specific VLAN:

```
switch# show mac-address-table mac-move vlan 10
Number of MAC Move addresses : 2
```

MAC Address	VLAN	Current Port	Previous Port	Move Count	Last Move
00:00:00:00:00:bb 19:11:52 2023	10	1/1/28	1/1/27	2	Fri Sep 15
00:00:00:00:00:aa 19:11:51 2023	10	1/1/27	1/1/28	2	Fri Sep 15

Showing the number MAC move addresses on a specific MAC address and VLAN:

```
switch# show mac-address-table mac-move address 00:00:00:00:00:aa vlan 10
Number of MAC Move addresses : 1
```

MAC Address	VLAN	Current Port	Previous Port	Move Count	Last Move
00:00:00:00:00:aa 19:11:51 2023	10	1/1/27	1/1/28	2	Fri Sep 15



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.13 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table port

show mac-address-table port <PORT-NUM> [vsx-peer]

Description

Shows the MAC address table entries for the specified port.

Parameter	Description
<PORT-NUM>	Specifies a physical port on the switch. Format: member/slot/port .
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the MAC address table entries for port **1/1/1**:

```
switch# show mac-address-table port 1/1/1
MAC age-time           : 300 seconds
Number of MAC addresses : 1

MAC Address            VLAN    Type      Port
-----
00:00:00:00:00:01     2      dynamic   1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager	Operators or Administrators or local user group members with

Platforms	Command context	Authority
	(#)	execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table static

show mac-address-table static

Description

Shows all statically configured MAC addresses.

Examples

```
switch# show mac-address-table static
Number of MAC addresses : 2

MAC Address          VLAN    Port
-----
00:00:00:00:10:02    1       1/1/1
00:00:00:00:10:03    1       1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-address-table vlan

show mac-address-table vlan <VLAN-ID> [vsx-peer]

Description

Shows MAC addresses learned by or configured on the specified VLAN.

Parameter	Description
vlan <VLAN-ID>	Specifies the VLAN ID.

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show mac-address-table vlan 1
MAC age-time           : 300 seconds
Number of MAC addresses : 1
```

MAC Address	VLAN	Type	Port
00:00:00:00:00:01	1	dynamic	1/1/1



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac address table mac move

```
show mac-address-table mac-move [address <mac-address> vlan <vlan>] | [vlan <vlan>]
```

Description

Displays the MAC entries in the MAC address table that have moved at least once. The output can be filtered based on a specific VLAN or specific MAC address and VLAN.

Parameter	Description
<code><address></code>	Displays information for a specific MAC address.
<code><vlan></code>	Displays information for specific VLANs.

Examples

Displaying the moved MAC addresses:

```
switch# show mac-address-table mac-move
Number of MAC addresses : 2
```

MAC Address	VLAN	Current Port	Previous Port	Move Count	Last Move
00:00:00:00:00:bb 19:11:52 2023	10	1/1/28	1/1/27	2	Fri Sep 15
00:00:00:00:00:aa 19:11:51 2023	10	1/1/27	1/1/28	2	Fri Sep 15

```
switch# show mac-address-table mac-move address 00:00:00:00:00:aa vlan 10
Number of MAC Move addresses : 1
```

MAC Address	VLAN	Current Port	Previous Port	Move Count	Last Move
00:00:00:00:00:aa 19:11:51 2023	10	1/1/27	1/1/28	2	Fri Sep 15

```
switch# show mac-address-table mac-move vlan 10
Number of MAC Move addresses : 2
```

MAC Address	VLAN	Current Port	Previous Port	Move Count	Last Move
00:00:00:00:00:bb 19:11:52 2023	10	1/1/28	1/1/27	2	Fri Sep 15
00:00:00:00:00:aa 19:11:51 2023	10	1/1/27	1/1/28	2	Fri Sep 15



In the case of MACs learned on VXLAN tunnels or "port-access port-security" enabled ports, the move scenario is handled by the EVPN/port-access feature respectively and it performs the move by deleting the MAC from the old port and installing it on the new port. Thus, the MAC move data will be removed for the deleted MAC addresses.

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

static-mac

```
static-mac
  <MAC-ADDR>
  vlan <VLAN-ID> port
```

```
<PORT-NUM>
workload
no...
```

Description

Adds a static MAC address to the MAC address table and associates it with a port or existing VLAN. Static MAC addresses can only be assigned to layer 2 (non-routed) interfaces. Static MAC addresses are not affected by the MAC address aging time.

The **no** form of this command deletes a static MAC address.

Parameter	Description
<MAC-ADDR>	Specifies a MAC address (xx:xx:xx:xx:xx:xx), where x is a hexadecimal number from 0 to F.
vlan <VLAN-ID>	Specifies number of an existing VLAN.
port <PORT-NUM>	Specifies a physical port on the switch. Format: member/slot/port .

Examples

```
switch(config)# static-mac 00:00:00:00:00:01 vlan 1 port 1/1/1
switch(config)# no static-mac 00:00:00:00:00:01 vlan 1 port 1/1/1

switch(config)# static-mac 00:00:00:00:00:01 vlan 1 port 1/1/2
1/1/2 is not an L2 port

switch(config)# static-mac 00:00:00:00:00:01 vlan 2 port 1/1/1
VLAN 2 not found
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

apply macsec policy

```
apply macsec policy <MACSEC-POLICY-NAME>
no apply macsec policy
```

Description

Within the selected interface context, applies the specified MACsec policy to the selected port. When a MACsec policy is applied to a port, MACsec is enabled on the port and all data traffic is blocked on the port until a secure channel is successfully established.



A MACsec policy can be applied to a physical interface port that is not part of any LAG ports or to a lag port. It can also be applied to an interface that is configured as an MCLAG, VSX keep-alive, or VSX inter-switch-link.

If a MACsec policy is already applied to the selected port, this command replaces the existing policy application.



For MACsec to work, an MKA policy must also be configured and applied to the same ports.

The **no** form of this command dissociates the specified policy from the port.

Parameter

Description

<MACSEC-POLICY-NAME>

Specifies the MACsec policy name. Range: 1 to 128 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Usage

- When any MACsec or MKA policy parameter is updated, any active MACsec session on all interfaces running the MACsec or MKA policy is terminated and restarted. This is indicated with the following prompt that provides an opportunity to not execute the **apply** command.

```
This policy is currently in use by one or more interfaces.
Updating the policy will cause existing MACsec sessions using
the policy to restart.
Continue (y/n)?
```

- For non-LAG ports, a range of ports can be specified in the **interface** command used to enter the interface context. For example, entering the interface context for ports 1/1/1 through 1/1/2:

```
switch(config)# interface 1/1/1-1/1/2
switch(config-if-<1/1/1-1/1/2>)# apply macsec policy MS_Policy1
```

- Not all interfaces on a switch may support the MACsec capability. An error will be generated when a policy is applied to a physical interface that is not capable of MACsec. For LAG ports, any non-MACsec capable interfaces that are part of the LAG will be blocked.

Examples

Applying a MACsec policy to a range of two ports:

```
switch(config)# interface 1/1/1-1/1/2
switch(config-if-<1/1/1-1/1/2>)# apply macsec policy MS_Policy1
```

Attempting to apply a MACsec policy to a port that is not MACsec capable:

```
9300(config)# int 1/1/9
9300(config-if)# apply macsec policy m1

MACsec is not supported on the interface.
```

Removing MACsec policy association from a port:

```
switch(config)# interface 1/1/1
switch(config-if)# no apply macsec policy
```

Applying a MACsec policy to a LAG port:

```
switch(config)# interface lag 1
switch(config-if)# apply macsec policy MS_Policy1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-if	Administrators or local user group members with execution rights for this command.

bypass

bypass {ieee-bpdu}

```
no bypass {ieee-bpdu}
```

Description

Configures the MACsec policy to bypass MACsec for specific features.

When bypass is enabled on the BPDU, packets with a destination MAC matching the IEEE BPDU MAC (01:80:c2:00:00:0*) will bypass MACsec on both the egress and ingress directions.

By default, when MACsec is enabled on an interface, all BPDU frames except EAPoL are protected by MACsec. However, when an interface configured is configured to initiate a MACsec tunnel, the BPDU frames that are essential to the next hop device are sent with MACsec protection. This causes protocols such as LLDP and LACP to fail on the local link since the next hop device will fail to read the MACsec protected frames. To enable these protocols to operate on such links, you must enable BPDU bypass in the MACsec policy.

The **no** form of the command disables MACsec bypass for the specified feature. When no feature is specified, MACsec bypass is disabled for all the features.

MACsec WAN extension is only supported on the following switches:

Platform	SKU	Interfaces
9300S	S0F96A	1/1/1 - 1/1/8, 1/1/33 - 1/1/40

Examples

Enabling the MACsec bypass for IEEE BPDUs:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# bypass ieee-bpdu
OR
switch(config)# macsec policy Aggregator-Connect bypass ieee-bpdu
```

Disabling the MACsec bypass for IEEE BPDU:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# no bypass ieee-bpdu
OR
switch(config)# no macsec policy Aggregator-Connect bypass ieee-bpdu
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

cipher-suite (MACsec)

```
cipher-suite {<CIPHER-SUITE>} [<CIPHER-SUITE>] ... [<CIPHER-SUITE>]
no cipher-suite [<CIPHER-SUITE>] ... [<CIPHER-SUITE>]
```

Description

Within the MACsec policy context, configures one or more cipher suites to be used to generate the SAK (Secure Authentication Key) for when the switch is the key server. When multiple cipher suites are configured, the most secure cipher suite is considered first during negotiation.

The no form of this command (without the **<CIPHER-SUITE>** parameter) resets to the default of considering (during negotiation) all supported cipher suites while giving priority to the most secure suite **gcm-aes-xpn-256**. Include the **<CIPHER-SUITE>** parameter to disable a particular cipher suite.

Parameter	Description
<CIPHER-SUITE>	Selects the cipher suite. Available cipher suites are: ▪ gcm-aes-128: AES-128 encryption with Galois/Counter mode. ▪ gcm-aes-256: AES-256 encryption with Galois/Counter mode. ▪ gcm-aes-xpn-128: AES-128 encryption with Galois/Counter mode and extended packet numbering. ▪ gcm-aes-xpn-256: AES-128 encryption with Galois/Counter mode and extended packet numbering. (The default and the most secure.)

Examples

Enabling a single cipher suite:

```
switch(config-macsec-policy)# cipher-suite gcm-aes-128
```

Enabling two cipher suites:

```
switch(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256
```

Disabling a particular cipher suite:

```
switch(config-macsec-policy)# no cipher suite gcm-aes-128
```

Resetting to the default of considering all available cipher suites while giving priority to **gcm-aes-xpn-256**:

```
switch(config-macsec-policy)# no cipher-suite
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-macsec-policy	Administrators or local user group members with execution rights for this command.

clear macsec statistics

```
clear macsec statistics [interface <IF-RANGE>]
```

Description

Clears MACsec statistics on all MACsec-enabled interfaces or on a specific interface or interface range. MACsec statistics are cleared for the entire switch rather than just in the current user session.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MACsec statistics information is to be cleared.

Examples

Clearing MACsec statistics on an interface range:

```
switch# clear macsec statistics interface 1/1/1-1/1/4
```

Clearing MACsec statistics on all MACsec-enabled interfaces:

```
switch# clear macsec statistics
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

clear tag mode

```
clear tag mode {dot1q | none}
no clear tag mode {dot1q | none}
```

Description

Configures the part of the Ethernet payload in a MACsec protected frame that must precede the Security TAG (SecTAG) header in clear text.

The **dot1q** mode allows the 802.1q tag of a MACsec protected frame to be sent in clear text and placed before the MACsec SecTAG header. This enables the establishment of a MACsec tunnel between two MACsec endpoints over a non-MACsec Layer 2 network.

The **no** form of the command will configure the device to place the SecTAG header immediately after the destination and source MAC addresses.

MACsec WAN extension is only supported on the following switches:

Platform	SKU	Interfaces
9300S	S0F96A	1/1/1 - 1/1/8, 1/1/33 - 1/1/40



Untagged traffic is not supported on a MACsec channel running clear-tag mode as **dot1q**. All untagged frames will be dropped on ingress.

Parameter	Description
dot1q	Specifies the encoding of a single 802.1q tag in clear text before Security TAG (SecTAG).
none	Specifies that the Security TAG (SecTAG) directly follows the Ethernet addresses. This is the default option.

Examples

Configuring the clear-tag mode as **dot1q**:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# clear-tag-mode dot1q
OR
switch(config)# macsec policy Aggregator-Connect clear-tag-mode dot1q
```

Resetting the clear-tag mode:

```
switch(config)# macsec policy Aggregator-Connect
switch(config-macsec-policy)# no clear-tag-mode dot1q
OR
switch(config)# no macsec policy Aggregator-Connect clear-tag-mode dot1q
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

confidentiality

```
confidentiality [offset {0|30|50}]
no confidentiality
```

Description

Within the MACsec policy context, enables Ethernet packet encryption after the MACsec header, optionally including a start-of-encryption offset. Confidentiality is enabled by default with an offset of 0 bytes after the MACsec header.

An offset of 0 causes the entire packet (after the MACsec header) to be encrypted. It is sometimes desirable to offset the start of the encryption deeper into the packet to allow for fields such as MPLS labels and 802.1Q tags to remain unencrypted.

Omitting the **offset** parameter enables confidentiality with whatever offset was configured previously. The **no** form of this command disables confidentiality.

Parameter	Description
offset {0 30 50}	Selects the start-of-encryption offset (in bytes) into the packet after the MACsec header. Default 0 bytes.

Examples

Enabling confidentiality with an offset of 30 bytes:

```
switch(config-macsec-policy)# confidentiality offset 30
```

Disabling confidentiality

```
switch(config-macsec-policy)# no confidentiality
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-macsec-policy	Administrators or local user group members with execution rights for this command.

include-sci-tag

```
include-sci-tag  
no include-sci-tag
```

Description

Within the MACsec policy context, enables inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header. This is the default.

Inclusion of the SCI tag is not required on point-to-point links if the transmitting link has only one MACsec peer.

The **no** form of this command disables inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header.

Examples

Enabling the SCI tag:

```
switch(config-macsec-policy)# include-sci-tag
```

Disabling the SCI tag:

```
switch(config-macsec-policy)# no include-sci-tag
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-macsec-policy	Administrators or local user group members with execution rights for this command.

macsec policy

```
macsec policy <MACSEC-POLICY-NAME>
no macsec policy <MACSEC-POLICY-NAME>
```

Description

Creates the specified MACsec policy and then enters its context (displayed in the CLI as **config-macsec-policy**). If the MACsec policy already exists, this command enters the specified MACsec policy context.

A MACsec policy can be applied to one or more switch ports, enabling MACsec on the ports. An MKA (MACsec Key Agreement) policy must be applied to the same ports.

The **no** form of this command deletes the MACsec policy.



A MACsec policy cannot be deleted if it is currently applied to any ports. All application of the policy must be removed before the policy can be deleted.

Parameter	Description
<MACSEC-POLICY-NAME>	Specifies the MACsec policy name. Range: 1 to 128 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Creating a MACsec policy:

```
switch(config)# macsec policy MS_Policy1
switch(config-macsec-policy)#
```

Deleting a MACsec policy (the policy cannot be currently applied to any ports):

```
switch(config)# no macsec policy MS_Policy1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config	Administrators or local user group members with execution rights for this command.

macsec selftest

```
macsec selftest
no macsec selftest
```

Description

Configures the system to run a self test for MACsec on all MACsec-capable interfaces.

The **no** form of the command disables the MACsec self test on the device.

When enabled, the system will drop traffic on all MACsec capable interfaces until the MACsec selftest completes successfully on the interface. A MACsec selftest will be run in the following scenarios:

- After every reboot (if enabled)

Examples

Running a MACsec self test:

```
switch(config)# macsec selftest
```

Disabling the MACsec self test:

```
switch(config)# no macsec selftest
```

Running a MACsec self-test from the switch user mode:

```
switch# macsec selftest run interface 1/1/1-1/1/4
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config	Administrators or local user group members with execution rights for this command.

replay-protection

```
replay-protection [window-size <WINDOW-SIZE>]
no replay-protection
```

Description

Within the MACsec policy context, enables replay protection with the default or specified window size. With replay protection enabled, packets are expected to arrive within the replay protection window number of packets. For example with a window size of 10, any packet arriving out-of-sequence by more than 10 packets will be discarded. A window size of 0 (the default) enforces strict order of packet reception, discarding all packets not received in perfect sequence.

The **no** form of this command disables replay protections and resets the window size to its 0 default.

Parameter	Description
<WINDOW-SIZE>	Specifies the replay protection window size in packets. Default 0 packets. Range: 0 to 4294967295 packets.

Examples

Enabling replay protection with the default window size of 0 (strict order of packet reception):

```
switch(config-macsec-policy) # replay-protection
```

Enabling replay protection with a windows size of 100 packets:

```
switch(config-macsec-policy) # replay-protection window-size 100
```

Disabling replay protection.

```
switch(config-macsec-policy) # no replay-protection
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-macsec-policy	Administrators or local user group members with execution rights for this command.

show macsec policy

```
show macsec policy [<MACSEC-POLICY-NAME>]
```

Description

Shows information for one or all MACsec policies.

Parameter	Description
<code><MACSEC-POLICY-NAME></code>	Specifies the MACsec policy name. Range: 1 to 128 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Showing information for a specific MACsec policy:

```
9300(config)# sh macsec policy

MACsec Policy Details
=====

Policy Name: m1
-----
Cipher suite           : GCM-AES-128, GCM-AES-256, GCM-AES-XPB-128, GCM-AES-XPB-
256
Include SCI            : Yes
Confidentiality        : Enabled
Confidentiality offset : 0
Replay protection      : Enabled
Replay protection window : 0
Data delay protection  : Disabled
Bypass                 :
Clear Tag Mode         : None
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show macsec selftest

```
show macsec selftest [interface <IFRANGE>]
```

Description

Shows the status of the MACsec selftest for MACsec capable interfaces. If an interface fails the self test then MACsec selftest should be disabled.

Parameter	Description
<IFRANGE>	Specifies the interface(s) for which to show MACsec selftest information.

Examples

Showing MACsec self test information for all interfaces that are MACsec capable:

```
switch# show macsec selftest
MACsec selftest status

Interface  Status      Failure Reason
-----
1/1/1     Initializing --
1/1/2     Passed      --
1/1/3     Queued for run --
1/1/4     Running
1/1/5     Failed      Encryption test failed
1/1/6     Failed      Decryption test failed
1/1/7     Failed      Initialization failed
1/1/8     Failed      Time out
```

Showing MACsec self test information for a specific interface:

```
switch# show macsec selftest interface 1/1/1
MACsec selftest status

Interface  Status  Failure Reason
-----
1/1/1     Passed  --
```

Showing MACsec self test information for an interface range:

```
switch# show macsec selftest interface 1/1/1-1/1/3
MACsec selftest status

Interface  Status      Failure Reason
-----
1/1/1     Passed      --
1/1/2     Running     --
1/1/3     Failed      Decryption test failed
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show macsec statistics

show macsec statistics [interface <IF-RANGE>]

Description

Shows MACsec statistics for all MACsec-enabled interfaces or a specific interface or interface range.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MACsec statistics information is to be shown.

Examples

Showing MACsec statistics for a specific interface:

```
switch# show macsec statistics interface 1/1/1

MACsec Statistics

Interface 1/1/1
=====

Rx Statistics
-----
Unicast Uncontrolled Packets      : 170438363226
Multicast Uncontrolled Packets    : 66586
Broadcast Uncontrolled Packets    : 4399
Rx Uncontrolled Drop Packets      : 0
Rx Uncontrolled Error Packets     : 0
Rx Controlled Unicast Packets     : 170438369232
Rx Controlled Multicast Packets   : 31298
Rx Controlled Broadcast Packets   : 4399
Rx Controlled Drop Packets        : 0
Rx Controlled Error Packets       : 0
Uncontrolled Octets               : 27270198219337
Controlled Octets                 : 21816165353719

Tx Statistics
-----
Unicast Uncontrolled Packets      : 0
Multicast Uncontrolled Packets    : 33756
Broadcast Uncontrolled Packets    : 0
Rx Uncontrolled Drop Packets      : 0
Rx Uncontrolled Error Packets     : 0
Unicast Controlled Packets       : 171226945517
Multicast Controlled Packets      : 98215
Broadcast Controlled Packets      : 71894
Rx Controlled Drop Packets        : 0
Rx Controlled Error Packets       : 0
Uncontrolled Octets              : 4658308
Controlled Octets                 : 21917110733304
Common Octets                     : 27396383670012
```

SecY Statistics

Port Identifier : 1

Rx Statistics

Transform Error Packets	: 0
Control Packets	: 35288
Untagged Packets	: 0
No Tag Packets	: 0
Bad Tag Packets	: 39
No SCI Packets	: 0
Unknown SCI Packets	: 0
Tagged Control Packets	: 0
Overrun Packets	: 0

Tx Statistics

Transform Error Packets	: 0
Control Packets	: 33756
Untagged Packets	: 0

Transmit Secure Channel

SCI : ec0273f72f4d0001

Statistics

Encrypted Packets	: 171227173728
Protected Packets	: 0

Secure Association

Association Number : 0

Statistics

Encrypted Packets	: 171227173728
Encrypted Octets	: 19862392663792
Protected Packets	: 0
Protected Octets	: 0
Too Long Packets	: 0
SA Not In Use Packets	: 0

Receive Secure Channel

SCI : 00fd4568f4110001

Statistics

Late Packets	: 0
Not Valid Packets	: 0
Delayed Packets	: 0
Ok Packets	: 170438441668

Secure Association

Association Number : 0

Statistics

```
Unchecked Packets      : 0
Delayed Packets        : 0
Late Packets           : 0
Ok Packets             : 170438441668
Invalid Packets        : 0
Not Valid Packets      : 0
Not Using SA Packets   : 0
Unused SA Packets      : 0
Decrypted Octets       : 19770908750641
Validated Octets       : 0
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show macsec status

```
show macsec status [interface <IF-RANGE>] [detailed]
```

Description

Shows MACsec status information for all MACsec-enabled interfaces or a specific interface or interface range.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MACsec status information is to be shown.
detailed	Specifies that detailed status information is to be shown.

Usage

Applicable to when the **detailed** parameter is included: The stop time for the MACsec secure channel and secure association is updated only when the secure channel or association entry is being deleted. Therefore, it is never shown as set in the **show macsec status detailed command** output.

Examples

Showing MACsec summary information for all interfaces:

```
switch# show macsec status
```

MACsec Protocol Status

Interface	Port ID	Policy	Protection	Status	State
1/1/1	0	MS_Policy1	Conf, Offset 0	Up	Retire
1/1/2	0	MS_Policy1	IC	Down	Init
...					

Showing detailed MACsec information for a specific interface:

```
9300(config)# show macsec status interface 1/1/4 detailed
```

MACsec Protocol Status

Interface 1/1/4

=====

Port Identifier: 1

=====

Policy : m1
Status : Up
State : Retire
Cipher Suite : GCM-AES-XPB-256
Protection : IC, Conf, Offset 0

Bypass : -
Clear Tag Mode : None
Transmit Secure Channel

SCI : e4de40bb2afd0001
SSCI : 1

Secure Association

Association Number : 0 (current)
Key Identifier : 168496150f5dde1e3c1ac18a00000001
Packet Number : 4
SA-Start-Time : Wed May 22 08:17:02 UTC 2024
SA-Stop-Time : -

Receive Secure Channel

SCI : e4de40bb17fc0001
SSCI : 2

Secure Association

Association Number : 0 (current)
Key Identifier : 168496150f5dde1e3c1ac18a00000001
Lowest Packet Number : 5
SA-Start-Time : Wed May 22 08:17:02 UTC 2024
SA-Stop-Time : -



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

default-gateway

```
default-gateway <IP-ADDR>
no default-gateway <IP-ADDR>
```

Description

Assigns an IPv4 or IPv6 default gateway to the management interface. An IPv4 default gateway can only be configured if a static IPv4 address was assigned to the management interface. An IPv6 default gateway can only be configured if a static IPv6 address was assigned to the management interface. The default gateway should be on the same network segment.

The **no** form of this command removes the default gateway from the management interface.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

Examples

Setting a default gateway with the IPv4 address of **198.168.5.1**:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# default-gateway 198.168.5.1
```

Setting an IPv6 address of **2001:DB8::1**:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# default-gateway 2001:DB8::1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-mgmt	Administrators or local user group members with execution rights for this command.

ip static

```
ip static <IP-ADDR>/<MASK>
no ip static <IP-ADDR>/<MASK>
```

Description

Assigns an IPv4 or IPv6 address to the management interface.

The **no** form of this command removes the IP address from the management interface and sets the interface to operate as a DHCP client.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<MASK>	Specifies the number of bits in an IPv4 or IPv6 address mask in CIDR format (x), where x is a decimal number from 0 to 32 for IPv4, and 0 to 128 for IPv6.

Examples

Setting an IPv4 address of **198.51.100.1** with a mask of **24** bits:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip static 198.51.100.1/24
```

Setting an IPv6 address of **2001:DB8::1** with a mask of **32** bits:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip static 2001:DB8::1/32
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-mgmt	Administrators or local user group members with execution rights for this command.

nameserver

```
nameserver <PRIMARY-IP-ADDR> [ <SECONDARY-IP-ADDR> ]
no nameserver <PRIMARY-IP-ADDR> [ <SECONDARY-IP-ADDR> ]
```

Description

Assigns a primary or secondary IPv4 or IPv6 DNS server to the management interface. IPv4 DNS servers can only be configured if a static IPv4 address was assigned to the management interface. IPv6 DNS servers can only be configured if a static IPv6 address was assigned to the management interface. The default gateway should be on the same network segment.

The **no** form of this command removes the DNS servers from the management interface.

Parameter	Description
<PRIMARY-IP-ADDR>	Specifies the IP address of the primary DNS server. Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<SECONDARY-IP-ADDR>	Specifies the IP address of the secondary DNS server. Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

Examples

Setting primary and secondary DNS servers with the IPv4 addresses of **198.168.5.1** and **198.168.5.2** :

```
switch(config)# interface mgmt
switch(config-if-mgmt)# nameserver 198.168.5.1 198.168.5.2
```

Setting primary and secondary DNS servers with the IPv6 addresses of **2001:DB8::1** and **2001:DB8::2**:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# nameserver 2001:DB8::1 2001:DB8::2
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-mgmt	Administrators or local user group members with execution rights for this command.

show interface mgmt

show interface mgmt [vsx-peer]

Description

Shows status and configuration information for the management interface.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show interface mgmt

Address Mode           : static
Admin State            : up
Mac Address            : 02:42:ac:11:00:02
IPv4 address/subnet-mask : 192.168.1.10/16
Default gateway IPv4    : 192.168.1.1
IPv6 address/prefix     : 2001:db8:0:1::129/64
IPv6 link local address/prefix: fe80::7272:cfff:fe485/64
Default gateway IPv6    : 2001:db8:0:1::1
Primary Nameserver      : 2001::1
Secondary Nameserver    : 2001::2
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

debug mdns

debug mdns {all | config | init | packet | timer}

Description

Enables mDNS gateway debug logs for all or specific debug modules.

Parameter	Description
all	Enables debug logs for all mDNS gateway modules.
config	Enables debug logs to trace mDNS gateway configuration changes.
init	Enables debug logs to trace mDNS gateway initialization.
packet	Enables debug logs to trace mDNS gateway packet processing.
timer	Enables debug logs to trace mDNS gateway timer events.

Examples

Enabling debug logs for all modules:

```
switch# debug mdns all
```

Enabling debug logs for config module:

```
switch# debug mdns config
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

description

```
description <SERVICE-DESCRIPTION>
no description <SERVICE-DESCRIPTION>
```

Description

Adds description to a service.

The **no** form of this command deletes the description of a service.

Parameter	Description
<SERVICE-DESCRIPTION>	Specifies the service description. Maximum 128 characters.

Examples

Add a service description:

```
switch(config-mdns-sd-service)# description students-airplay-service
```

Remove the service description from a service:

```
switch(config-mdns-sd-service)# no description students-airplay-service
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-mdns-sd-service	Administrators or local user group members with execution rights for this command.

id

```
id <SERVICE-ID>
no id <SERVICE-ID>
```

Description

Adds a service identifier to a service. The service ID configured here must be same as the service ID that is present in the packet.

The **no** form of this command removes a service ID from the service.

Parameter	Description
<code><SERVICE-ID></code>	Specifies the service ID. Maximum 128 characters.

Examples

Add a service ID:

```
switch(config-mdns-sd-service)# id _appletv-v2._tcp
```

Remove a service ID from a service:

```
switch(config-mdns-sd-service)# no id _appletv-v2._tcp
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-mdns-sd-service	Administrators or local user group members with execution rights for this command.

mdns-sd

mdns-sd
no mdns-sd

Description

Enables mDNS gateway on a VLAN interface.

The **no** form of this command disables mDNS gateway on a VLAN interface.



This command is applicable only to VLAN interfaces.

The switch will not process mDNS packets until the mDNS gateway is enabled globally.

Examples

Enabling mDNS gateway on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# mdns-sd
```

Disabling mDNS gateway on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no mdns-sd
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

mdns-sd apply-profile tx

```
mdns-sd apply-profile <PROFILE-NAME> tx
no mdns-sd apply-profile <PROFILE-NAME> tx
```

Description

Configures mDNS gateway profile on the VLAN interface. When a profile is applied in the transmit direction, all the mDNS traffic transmitted on the VLAN interface will be filtered based on the rules specified in the transmit profile.

The **no** form of this command deletes the profile configuration from the VLAN interface in the transmit direction.



This command is applicable only to VLAN interfaces.
When no profile is configured on an interface then the default action is permit.

Parameter	Description
<PROFILE-NAME>	Specifies the profile name. Maximum 32 characters.

Examples

Configuring mDNS gateway profile on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# mdns-sd
switch(config-if-vlan)# mdns-sd apply-profile student tx
```

Deleting mDNS gateway profile on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no mdns-sd apply-profile student tx
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

mdns-sd enable

```
mdns-sd enable
no mdns-sd enable
```

Description

Enables mDNS gateway.

The **no** form of this command disables mDNS gateway. Once the **no** form of this command is executed, all the SVI VLANs, even though enabled with mDNS gateway, will stop reflecting mDNS packets to the enabled VLANs.

Examples

Enable mDNS gateway:

```
switch(config)# mdns-sd enable
```

Disable mDNS gateway:

```
switch(config)# no mdns-sd enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

mdns-sd profile

mdns-sd profile <PROFILE-NAME>

Description

Creates a profile that can be applied on one or more L3 VLAN interfaces.

The profile contains a set of rules that define various match parameters such as service-name and service-instance-name.

Parameter	Description
<PROFILE-NAME>	Specifies the name of the profile. Maximum 32 characters.

Examples

Creating a profile:

```
switch(config)# mdns-sd profile student
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

mdns-sd service

```
mdns-sd service <SERVICE-NAME>
no mdns-sd service
```

Description

Configures a service for mDNS gateway. You can group multiple service IDs into a single user-defined service name.

The **no** form of this command deletes a service.



A service cannot be deleted if it is being used as a match parameter in a filter rule in any profile.

Parameter	Description

<SERVICE-NAME>	Specifies the name of the service. Maximum 32 characters.

Examples

Configure a service for mDNS gateway:

```
switch(config)# mdns-sd service students
```

Delete a service:

```
switch(config)# no mdns-sd service students
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification

10.07 or earlier	--

Command Information

Platforms	Command context	Authority

9300 9300S	config	Administrators or local user group members with execution rights for this command.

clear mdns-sd statistics

```
clear mdns-sd statistics
```

Description

Clears all mDNS gateway statistics.

Examples

Clear mDNS gateway statistics:

```
switch(config)# clear mdns-sd statistics
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

sequence-number

```
<SEQUENCE_NUMBER> {permit | deny}
{service-name <SERVICE-NAME> | service-instance-name <SERVICE-INSTANCE-NAME>}
no <SEQUENCE_NUMBER> {permit | deny}
{service-name <SERVICE-NAME> | service-instance-name <SERVICE-INSTANCE-NAME>}
```

Description

Adds a filter rule to the service profile. The sequence number configured determines the priority with which the rule is matched. Lower the sequence number, higher is the priority.

Following are the filter match parameters:

- **Service-name:** mDNS packets are matched against the service IDs configured under the service name.
- **Service-instance-name:** mDNS packets are matched against the service instance name present in the mDNS packets.

When no match criteria is specified in the rule, then the rule can be matched against any mDNS packet. Once the match is found then either the packet can be permitted or denied based on the action specified in the rule.

The **no** form of this command deletes the filter configured in the service profile.



When an mDNS packet does not match any of the filters configured in the profile, then the packet is denied.

Parameter	Description
<SERVICE-NAME>	Specifies the service name. Maximum 32 characters.
<SERVICE-INSTANCE-NAME>	Specifies the service instance name. Maximum 128 characters.

Examples

Adding filter rules to a service profile:

```
switch(config)# mdns-sd profile student
switch(config-mdns-sd-profile)# 10 permit service-name default-appletv
switch(config-mdns-sd-profile)# 20 deny service-name default-appletv service-
instance-name office._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 30 permit service-instance-name library._pdl-
datastream._tcp.local
switch(config-mdns-sd-profile)# 40 deny
```

Deleting filter rules to a service profile:

```
switch(config)# mdns-sd profile student
switch(config-mdns-sd-profile)# 10 permit service-name default-appletv
switch(config-mdns-sd-profile)# 20 deny service-name default-appletv service-
instance-name office._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 30 permit service-instance-name library._pdl-
datastream._tcp.local
switch(config-mdns-sd-profile)# no 30 permit service-instance-name library._pdl-
datastream._tcp.local
switch(config-mdns-sd-profile)# 40 deny
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-mdns-sd-profile	Administrators or local user group members with execution rights for this command.

show mdns-sd service-entries

```
show mdns-sd service-entries {service-id <SERVICE-ID> | record-type <RECORD-TYPE>}
```

Description

Shows all the services exchanged in the mDNS gateway enabled VLANs.

Parameter	Description
<SERVICE-ID>	Specifies the service ID. Maximum 128 characters
<RECORD-TYPE>	Specifies the type of record. Record can be one of the following values: PTR

Parameter	Description
	SRV TXT A

Examples

Displaying service entries learnt from mDNS gateway enabled VLANs:

```
switch# show mdns-sd service-entries
MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name  : _touch-able._tcp.local
Record Type  : PTR
TTL         : 4500

MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name  : 523899E219D4C562._touch-able._tcp.local
Record Type  : SRV
TTL         : 4500

MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name  : 523899E219D4C562._touch-able._tcp.local
Record Type  : TXT
TTL         : 4500
```

Displaying service entries for a service and record type:

```
switch# show mdns-sd service-entries service-id _touch-able._tcp record-type ptr
MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name  : _touch-able._tcp.local
Record Type  : PTR
TTL         : 4500
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mdns-sd statistics

show mdns-sd statistics [vlan [<VLAN-ID>]]

Description

Shows the mDNS packets received and sent globally, and per VLAN.

Parameter	Description
<VLAN-ID>	Specifies the VLAN ID. Required. Range 1 to 4094.

Examples

Displays total packets:

```
switch# show mdns-sd statistics
Packets Recieved      : 100
Packets Sent          : 150
Packets Dropped       : 50
```

Displays total packets for all VLANs:

```
switch# show mdns-sd statistics vlan
VLAN 10
Packets Recieved      : 100
Packets Sent          : 100
Packets Dropped       : 0

VLAN 20
Packets Recieved      : 0
Packets Sent          : 50
Packets Dropped       : 50
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mdns-sd statistics profile

show mdns-sd statistics profile <PROFILE-NAME>

Description

Displays the number of packets permitted or denied by various filter rules in a profile.

Parameter	Description
<code><PROFILE-NAME></code>	Specifies the profile name. Maximum 32 characters.

Examples

Displaying statistics for a profile:

```
switch# show mdns-sd statistics profile student
-----
Sequence-Number Hit-Count
-----
10                100
20                 25
30               150

Total number of packets permitted by the profile : 250
Total number of packets denied by the profile   :  50
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mdns-sd summary

`show mdns-sd summary`

Description

Shows whether mDNS gateway is enabled globally and at the VLAN interface level. It also shows the profile applied on various VLAN interfaces.

Examples

Displaying mDNS gateway summary:

```
switch# show mdns-sd summary
global mdns-sd status: enabled
-----
VLAN-Id  Status    Tx-Profile
-----
1         enabled    student
2         enabled    employee
3         disabled   teacher
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config interface

show running-config interface <INTERFACE-NAME>

Description

Shows the configuration of profiles for an interface.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.

Examples

Displaying configuration of profile at VLAN 10:

```
switch# show running-config interface vlan10
interface vlan10
  mdns-sd
  mdns-sd apply-profile teacher tx
  ip address 10.1.1.1/24
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config mdns-sd profile

show running-config mdns-sd profile <PROFILE-NAME>

Description

Shows the configuration of all or a specific profile.

Parameter	Description
<PROFILE-NAME>	Specifies the profile name. Maximum 32 characters.

Examples

Displaying configuration of all profiles:

```
switch# show running-config mdns-sd profile
mdns-sd profile student
  10 deny service-type default-print service-instance-name office._pdl-
  datastream._tcp.local
  50 permit service-type default-airplay
  51 permit service-type default-print

mdns-sd profile teacher
  10 deny service-type default-print service-instance-name office._pdl-
  datastream._tcp.local
  50 permit service-type default-airplay
  51 permit service-type default-print
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config mdns-sd service

show running-config mdns-sd service <SERVICE-NAME>

Description

Shows the running configuration of all or a specific mDNS service.

Parameter	Description
<SERVICE-NAME>	Specifies the service name. Maximum 32 characters.

Examples

Displaying running configuration of all mDNS services:

```
switch# show running-config mdns-sd service
mdns-sd service default-airplay
  id _airplay._tcp
  id _appletv-v2._tcp
  id _roap._tcp

mdns-sd service itunes
  id _home-sharing._tcp
  id _apple-mobdev._dev
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear mirror

clear mirror [all | <SESSION-ID>]

Description

Clears the mirror statistics for all configured mirror sessions or a specified session

Parameter	Description
all	Specifies all configured sessions.
<SESSION-ID>	Specifies a numeric identifier for the session. Range: 1 to 4

Examples

Clearing mirror statistics for all configured mirror sessions:

```
switch# clear mirror all
```

Clearing mirror statistics for mirror session 1:

```
switch# clear mirror 1
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

comment

comment <COMMENT>

no comment

Description

Specifies a comment for the mirroring session.

The **no** form of this command removes the comment.

Parameter	Description
<code><COMMENT></code>	A comment string of up to 64 characters composed of letters, numbers, underscores, dashes, spaces, and periods.

Usage

Comments are optional and can be added or removed at any time without affecting the state of the mirroring session.

Adding a comment to a session that already has a comment replaces the existing comment.

Examples

Adding a comment to a mirror session:

```
switch(config-mirror-3) # comment This Mirror will be removed during next  
maintenance window
```

Removing the comment from mirror session 3:

```
switch(config-mirror-3) # no comment
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-mirror-<SESSION-ID></code>	Administrators or local user group members with execution rights for this command.

copy tcpdump-pcap

`copy tcpdump-pcap <FILE-NAME> <REMOTE-URL>`

Description

Saves packet capture files to external storage.

Parameter	Description
<FILE-NAME>	Specifies the packet capture file to save.
<REMOTE-URL>	Specifies the external storage to which the packet capture file will be saved.

Usage

Only four files can be saved at any point on the switch. Packet capture files are not saved after a failover or reboot. View a list of saved files using **diag utilities list-files**.

Examples

Saving my_capture_file.pcap to sftp://root@10.0.0.2/file.pcap:

```
switch# copy tcpdump-pcap my_capture_file.pcap sftp://root@10.0.0.2/file.pcap
root@10.0.0.2's passwd:
Connected to 10.0.0.2.
sftp > put my_capture_file.pcap file.pcap
Uploading my_capture_file.pcap to /root/file.pcap
my_capture_file.pcap          100%   156   219.8KB/s   00:00
Copied successfully.
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

copy tshark-pcap

copy tshark-pcap <REMOTE-URL> [vrf <VRF-NAME>]

Description

Copies the tshark capture data to a file on a TFTP or SFTP server.

Parameter	Description
<REMOTE-URL>	Specifies the capture file on a remote TFTP or SFTP server. The URL syntax is: {tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>]

Parameter	Description
	[;blocksize=<SIZE>]/<FILE>
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Copying the capture data to a file on SFTP server 10.0.0.2:

```
switch# copy tshark-pcap sftp://root@10.0.0.2/file.pcap

root@10.0.0.2's password:
Connected to 10.0.0.2.
sftp> put packets.pcap file.pcap
Uploading packets.pcap to /root/file.pcap
packets.pcap                               100% 156   219.8KB/s   00:00
Copied successfully.
```



For more information on features that use this command, refer to the [Monitoring Guide](#) for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

destination cpu

```
destination cpu
no destination cpu
```

Description

The command causes the mirror session to transmit mirrored packets to the switch CPU. This destination may be configured for multiple sessions, however only one such configured session may be active at a given time.

The diagnostic utility Tshark may be used to view and capture packets transmitted to the CPU through this route. Ctrl+C must be entered to terminate a Tshark capture session. More details can be found in the **Supportability Guide**.

The **no** form of this command will immediately stops mirroring traffic to the CPU, but will not remove any sources from the mirror configuration.

Examples

Configuring a mirror session with CPU as the destination.

```
switch# config  
switch(config)# mirror session 1  
switch(config-mirror-1)# destination cpu
```

Removing the destination entirely.

```
switch(config-mirror-1)# no destination cpu
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-mirror- <i><SESSION-ID></i>	Administrators or local user group members with execution rights for this command.

destination interface

```
destination interface {<INTERFACE-ID>|<LAG-NAME>}  
no destination interface {<INTERFACE-ID>|<LAG-NAME>}
```

Description

Configures the specified interface as the destination of the mirrored traffic.

The **no** form of this command immediately disables the mirroring session and removes the specified destination interface from the configuration.

Parameter	Description
<i><INTERFACE-ID></i>	Specifies a interface. Format: member/slot/port.
<i><LAG-NAME></i>	Specifies a LAG (link aggregation group) identifier.

Usage

Configuring a different destination interface in an enabled mirroring session causes all mirrored traffic to use the new destination interface. This action might cause a temporary suspension of mirrored source traffic during the reconfiguration. Mirroring traffic to a LAG destination with a device running LACP attached to the destination will cause the LAG link to flap if LACP packets are part of the mirrored traffic source.

Examples

Configuring a mirroring session and adding an interface as a destination:

```
switch(config)# mirror session 1
switch(config-mirror-1)# destination interface 1/1/1
```

Replacing the existing destination with different interface:

```
switch(config-mirror-1)# destination interface 1/1/12
```

Removing a destination:

```
switch(config-mirror-1)# no destination interface 1/1/12
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Switch	Destination interface limit per mirror session (4 possible sessions)
9300/9300S	1

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror-<SESSION-ID>	Administrators or local user group members with execution rights for this command.

destination tunnel

```
destination tunnel <TUNNEL-IPV4> source <SOURCE-IPv4-ADDR>
dscp <DSCP-VALUE> vrf <VRF-NAME>
no destination tunnel
```

Description

Specifies the tunnel where all mirrored traffic for the session is transmitted. Only one tunnel destination is allowed per session.

You may configure multiple mirror sessions with the same source/destination IP address pair, however, only one of those sessions sharing the same source/destination IP address pair can be enabled at a given time.

ERSPAN is not supported leaving the switch by the OOB port. If VRF management is configured for an ERSPAN session, the session will be in "mirror_err_tunnel_oob_port_not_supported" operation status. ERSPAN is not supported leaving the switch encapsulated within another tunnel (e.g. GRE IPv4). When the path to the destination IP address will leave via a tunnel, the session will be in "tunnel_route_resolution_not_populated" operation status.



The interface/LAG used to transmit ERSPAN packets should not be a source in the same mirror session.

The **no** form of this command will cease the use of the tunnel and disable the session.

Parameter	Description
<TUNNEL-IPv4-ADDR>	Specifies the tunnel address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<SOURCE-IPv4-ADDR>	Specifies the source address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<DSCP-VALUE>	Specifies the DSCP value to be carried within the DS field of ERSPAN packet header. Range: 0 to 63. Default: 0.
<VRF-NAME>	Specifies a VRF name. Default: default.

Examples

Creating a Mirror Session and adding tunnel destination, source, dscp, and VRF:

```
switch# config
switch(config)# mirror session 1
switch(config-mirror-1)# destination tunnel 1.1.1.1 source 2.2.2.2 dscp 10 vrf
default
```

Replacing the existing tunnel destination:

```
switch(config-mirror-1)# destination tunnel 11.12.13.14 source 2.2.2.2 dscp 10 vrf
default
```

Replacing the existing destination with a different DSCP value:

```
switch(config-mirror-1)# destination tunnel 11.12.13.14 source 2.2.2.2 dscp 2 vrf
default
```

Removing the destination:

```
switch(config-mirror-1)# no destination tunnel
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-mirror-<SESSION-ID>	Administrators or local user group members with execution rights for this command.

diagnostic

diagnostic

```
diag utilities tshark [file]
diag utilities tshark [delete-file]
```

Description

Captures packets from a mirror-to-cpu session, and save the most recent 32MB to pcap file which can then be copied and analyzed. When capturing a mirror-to-cpu session to a file, packets will not be dumped to the console.



The **diagnostic** command must be entered prior to the **diag utilities tshark** command.

Use the **delete-file** form of this command to delete the most recent capture file.

Since **file** and **delete-file** are optional, the behavior of the base command **diag utilities tshark** does **not** save anything to a file, and instead dumps the tshark session to the console until **CTRL + c** is entered.

Parameter	Description
file	Saves captured packets to a temporary file.
delete-file	Deletes the most recent captured file.

Example

Performing diagnostic:

```
switch# diagnostic

switch# diagnostic utilities tshark file
Inspecting traffic mirrored to the CPU until Ctrl-C is entered
^CEnding traffic inspection.
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

diag utilities tcpdump

```
diag utilities tcpdump [command <TEXT> | delete file <FILE-NAME> | list-files |
vrf <VRF-NAME> | count <COUNT-NUM> | proto <PROTO-NUM> | host-ip <IP-ADDR> | source-ip
<IP-ADDR> | destination-ip <IP-ADDR> | host-port <PORT> | source-port <PORT> |
destination-port <PORT> | verbosity <LEVEL> | print <DATA> | ethernet-type <ETH-NUM>]
```

Description

Captures traffic received or transmitted over a network.

Parameter	Description
command <TEXT>	Captures packets based on a specified tcpdump command string.
delete file <FILE-NAME>	Deletes specified tcpdump list files.
list-files	Lists all the tcpdump capture files saved on the device.
vrf <VRF-NAME>	Captures packets on the specified VRF. If no VRF is named, the default is used.
count <COUNT-NUM>	Runs the tcpdump command until the specified number of packets are captured. Range: 1-2147483647.
proto <PROTO-NUM>	Captures packets of a particular type based on IP protocol number. Range: 0-255.
host-ip <IP-ADDR>	Captures packets matching with the source or destination IP address.
source-ip <IP-ADDR>	Captures packets from the specified IP address.
destination-ip <IP-ADDR>	Captures packets sent to the specified IP address.
host-port <PORT>	Captures packets matching with the source or destination port.
source-port <PORT>	Captures packets from the specified IP port.
destination-port <PORT>	Captures packets sent to the specified IP port.
verbosity <LEVEL>	Captures packets of the specified verbosity. Range: level1-level4. If no verbosity is specified, the default is level1.
print <DATA>	Captures the data of each packet. The maximum is 262144 bytes

Parameter	Description
<code>ethernet-type <ETH-NUM></code>	Captures packets based on the particular ethernet type. Range: 0-65535.

Usage

- When using the **command** option, the only traffic captured will be packets that have been mirrored to the CPU.
- When using the **command** option, command line sanitization is performed to prevent options that may cause harm or security issues. The following options are blocked:
 - `-i/--interface`
 - `-Z`
 - `-B/--buffer-size`
 - `-C`
 - `-W`
 - `-Z/--relinquish privileges`
- Non-word operators such as "&" or "|" are not allowed. Use boolean keywords such as "and," "or," and "not."
- When using **command -r** to read a file, do not provide any directory path characters. Use `list-files` command to get the list of file names currently saved on the device, and then use those file names.
- A total of four files can be saved at any given point on the device. Packet capture files are not saved after a failover or reboot, but can be saved to external storage using the **copy tcpdump-pcap** command.

Examples

Inspecting traffic mirrored to the CPU via tcpdump and saving the output to `my_capture_file.pcap`:

```
switch# diag utilities tcpdump command -c 2 -x -w my_capture_file.pcap
Inspecting traffic mirrored to the CPU via tcpdump until Ctrl-C is entered.
2 packets captured
2 packets received by filter
0 packets dropped by kernel
Ending traffic capture.
```

Listing saved capture files:

```
switch# diag utilities tcpdump list-files
my_capture_file.pcap
```

Reading `my_capture_file.pcap`:

```
switch# diag utilities tcpdump command -r my_capture_file.pcap
reading from file /tmp/tcpdump/my_capture_file1.pcap, link-type EN10MB (Ethernet)
1  11:59:34.047867 IP6 localhost.40318 > localhost.ntp: NTPv2, Reserved, length
12
    0x0000:  0000 0304 0006 0000 0000 0000 0000 86dd  .....
    0x0010:  600a 7e47 0014 1140 0000 0000 0000 0000  `..~G...@.....
    0x0020:  0000 0000 0000 0001 0000 0000 0000 0000  .....
```

```

0x0030:  0000 0000 0000 0001 9d7e 007b 0014 0027  .....~.{...
0x0040:  1601 0001 0000 0000 0000 0000                .....
2  11:59:34.047915 IP6 localhost.ntp > localhost.40318: NTPv2, Reserved, length
12
0x0000:  0000 0304 0006 0000 0000 0000 0000 86dd  .....
0x0010:  6b8d 23c5 0014 1140 0000 0000 0000 0000  k.#....@.....
0x0020:  0000 0000 0000 0001 0000 0000 0000 0000  .....
0x0030:  0000 0000 0000 0001 007b 9d7e 0014 0027  .....{.~...
0x0040:  d681 0001 c016 0000 0000 0000                .....

```

Removing my_capture_file.pcap:

```

switch# diag utilities tcpdump delete-file my_capture_file.pcap
Successfully removed file

```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables the mirroring session specified by the current command context.

Usage

By default, mirroring sessions are disabled.

When a mirroring session is disabled, the **show mirror** command for that session ID shows an **Admin Status** of **disable** and an **Operation Status** of **disabled**.

Example

Disabling a mirroring session:

```

switch(config)# mirror session 3
switch(config-mirror-3)# disable

```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror- <i><SESSION-ID></i>	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables the mirroring session for the current command context.

Usage

By default, mirroring sessions are disabled.

When a mirroring session is enabled, the **show mirror** command for that session ID shows an **Admin Status** of **enable** and an **Operation Status** of **enabled**.

If sFlow is enabled on an interface and a mirroring session specifies the same interface as the source of received traffic (the source is configured with a direction of **rx** or **both**):

- The attempt to enable the mirroring session fails and an error is returned.



When adding, removing, or changing the configuration of a source interface in an enabled mirroring session, packets from other mirror sources using the same destination interface might be interrupted.

Example

Configuring and enabling a mirroring session:

```
switch(config)# mirror session 3
switch(config-mirror-3)# source interface 1/1/2 rx
switch(config-mirror-3)# destination interface 1/1/3
switch(config-mirror-3)# comment Monitor router port ingress-only traffic
switch(config-mirror-3)# enable
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror- <i><SESSION-ID></i>	Administrators or local user group members with execution rights for this command.

mirror session

```
mirror session <SESSION-ID>
no mirror session <SESSION-ID>
```

Description

Creates a mirroring session configuration context or enters an existing mirroring session configuration context.

From this context, you can enter commands to configure and enable or disable the mirroring session. The **no** form of this command removes an existing mirroring session from the configuration.

Parameter	Description
<i><SESSION-ID></i>	Specifies the session identifier. Range: 1 to 4

Examples

```
switch(config)# mirror session 1
switch(config-mirror-1)#

switch(config)# mirror session 3
switch(config-mirror-3)#

switch(config)# no mirror session 1
switch(config)#
```



When configuring mirroring via the command-line interface, not all configuration errors will result in an immediate error message. After making configuration changes, always check the operation status of your mirror sessions using the **show mirror** command.



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show mirror

```
show mirror [<SESSION-ID>] [vsx-peer]
```

Description

Shows information about mirroring sessions. If **<SESSION-ID>** is not specified, then the command shows a summary of all configured mirroring sessions. If **<SESSION-ID>** is specified, then the command shows detailed information about the specified mirroring session.

Parameter	Description
<SESSION-ID>	Specifies the session identifier. Range: 1 to 4
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Information in the **Admin Status** column of the command output indicates the configured status. The admin status is one of the following values:

- **enable**: The mirroring session is enabled.
- **disable**: The mirroring session has been configured but not yet enabled, or has been disabled.

Information in the **Operation Status** column indicates the status of the mirroring session. Operation status is one of the following values:

- **dest_doesnt_exist**: The configured destination interface is not found in the system. The mirroring session cannot be enabled.
- **destination_shutdown**: **The mirroring session is enabled, but the destination interface is shut down. No traffic** can be monitored.
- **disabled**: The mirroring session is disabled and is not in an error condition.
- **enabled**: The mirroring session is enabled.
- **external/driver_error**: An internal ASIC hardware error occurred.
- **hit_active_sessions_capacity**: The mirroring session could not be enabled because the maximum number of supported mirroring sessions are already enabled.
- **internal_error**: An invalid parameter was passed to the ASIC software layer.
- **no_dest_configured**: The mirroring session does not have a destination interface configured.
- **no_name_configured**: A software error occurred. The mirroring session does not have a session ID in its configuration.
- **null_mirror**: A software error occurred. The session object reference is invalid.

- **out_of_memory:** The system is out of memory, reboot recommended.
- **tunnel_route_resolution_not_populated:** If the destination tunnel IP address is not reachable.
- **unknown_error:** An unexpected error occurred.

Examples

Showing summary information about all configured mirroring sessions:

```
switch# show mirror
ID   Admin Status   Operation Status
---   -
1    enable         enabled
2    disable        disabled
3    disable        disabled
4    enable         internal_error
```

Showing detailed information about a single mirroring session:

```
switch# show mirror 3
Mirror Session: 3
Admin Status: disable
Operation Status: disabled
Comment: Monitor router port ingress-only traffic
Source: interface 1/1/2 rx
Destination: interface 1/1/3
switch#
```

Show the details of mirror session 1 with an empty LAG as destination:

```
switch: show mirror 1
Admin Status: enable
Operation Status: dest_doesnt_exist
Source: interface 1/1/1 rx
Source: interface tx none
Destination: interface lag1
Output Packets: 0
Output Bytes: 0
```

Show the details of mirror session 1 with a LAG and a LAG member of same LAG as sources. In this scenario, traffic received on all LAG member interfaces is mirrored, is it is not necessary to define 1/1/1 as a source since it is already part of LAG1; this does not impact the mirror output packet or byte counters.

```
switch: show mirror 1
Admin Status: enable
Operation Status: enabled
Source: interface 1/1/1 rx
Source: interface lag1 rx
Destination: interface 1/1/2
Output Packets: 0
Output Bytes: 0
```

Showing the details of mirror **session 1** for a mirror configuration enabled with invalid interface which is not part of a lag:

```
switch# show mirror 1
Mirror Session: 1
Admin Status: enable
Operation Status: disabled
Source: interface 1/1/1 (unknown lag) both
Destination: cpu
Output Packets: 0
Output Bytes: 0
```

Certain configurations can cause this condition while the mirror source configuration remains unchanged:

1. Removing of a port from a LAG (Link Aggregation Group).
2. Port **split** or **unsplit** operations that result in LAG membership removal.

To recover from this issue, unconfigure the affected interface (previously part of a LAG), then restore the LAG membership configuration.



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

source interface

```
source interface {<PORT-NUM> | <LAG-NAME>} [<DIRECTION>]
no source interface {<PORT-NUM> | <LAG-NAME>} [<DIRECTION>]
```

Description

Configures the specified interface (either an Ethernet port or a LAG) as a source of traffic to be mirrored. The **no** form of this command ceases mirroring traffic from the specified source interface and removes the source interface from the mirroring session configuration.

Parameter	Description
<PORT-NUM>	Specifies a physical port on the switch. Use the format member/slot/port (for example, 1/3/1).
<LAG-NAME>	Specifies the identifier for the LAG (link aggregation group).

Parameter	Description
<DIRECTION>	Selects the direction of traffic to be mirrored from this source interface. There is no default for this parameter. Valid values are the following: - both: Mirror both transmitted and received packets. - rx: Mirror only received packets. - tx: Mirror only transmitted packets.

Usage

There is a limit of source interfaces in each direction of a given mirror session:

Switch	Source interface limit per mirror session (4 possible sessions)
9300/9300S	128
10000	72

However, there is a practical limit to the amount of traffic that a mirror destination can transmit. For example, mirroring session with multiple 10G sources can overwhelm a single 10G destination.

You can configure the same source interface in multiple mirroring sessions, if required.



When adding, removing, or changing the configuration of a source port in an enabled mirroring session, packets from other mirror sources using the same destination port might be interrupted.

Examples

Configuring a mirrored traffic source interface:

```
switch(config-mirror-1) # source interface
LAG-NAME      Enter a LAG name. For example, lag10
PORT-NUM      Enter a port number
```

Creating a mirroring session and configuring a source interface to mirror both transmitted and received packets:

```
switch(config) # mirror session 1
switch(config-mirror-1) # source interface 1/1/1 both
```

Creating a second mirroring session and configuring two source interfaces. One port mirroring only transmitted packets and the other mirroring both transmitted and received packets:

```
switch(config) # mirror session 2
switch(config-mirror-2) # source interface 1/1/3 tx
switch(config-mirror-2) # source interface 1/2/1 both
```

Removing the first source interface:

```
switch(config-mirror-2) # no source interface 1/2/3
```

Configuring a source interface to mirror received packets only:

```
switch(config-mirror-3) # source interface 1/1/2 rx
```

Configuring a source interface to mirror both transmitted and received packets:

```
switch(config-mirror-1) # source interface 1/1/1 both
```

Configuring a LAG as source interface to mirror both transmitted and received packets:

```
switch(config-mirror-4) # source interface lag1 both
```

Stopping the mirroring of received packets from a configured source interface:

```
switch(config-mirror-4) # no source interface lag1 rx
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror- <i><SESSION-ID></i>	Administrators or local user group members with execution rights for this command.

apply mka policy

```
apply mka policy <MKA-POLICY-NAME>
no apply mka policy
```

Description

Within the selected interface context, applies the specified MKA policy to the selected port. To start the MKA protocol on the port, a MACsec policy must also be applied to the port.



An MKA policy can be applied to a physical interface port that is not part of any LAG ports or to a lag port. It can also be applied to an interface that is configured as an MCLAG, VSX keep-alive, or VSX inter-switch-link.

If an MKA policy is already applied to the selected port, this command replaces the existing policy application.

The **no** form of this command dissociates the specified policy from the port.

Parameter	Description
<MKA-POLICY-NAME>	Specifies the MKA policy name. Range: 1 to 32 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Usage

- When any MACsec or MKA policy parameter is updated, any active MACsec session on all interfaces running the MACsec or MKA policy is terminated and restarted. This is indicated with the following prompt that provides an opportunity to not execute the **apply** command.

```
This policy is currently in use by one or more interfaces.
Updating the policy will cause existing MACsec sessions using
the policy to restart.
Continue (y/n)?
```

- For non-LAG ports, a range of ports can be specified in the **interface** command used to enter the interface context. For example, entering the interface context for ports 1/1/1 through 1/1/4:

```
switch(config)# interface 1/1/1-1/1/4
switch(config-if-<1/1/1-1/1/4>)# apply mka policy MKA_Policy1
```

- Not all interfaces on a switch may support the MACsec capability. An error will be generated when a policy is applied to a physical interface that is not capable of MACsec. For LAG ports, any non-MACsec capable interfaces that are part of the LAG will be blocked.

Examples

Applying an MKA policy to a range of two ports:

```
switch(config)# interface 1/1/1-1/1/2
switch(config-if-<1/1/1-1/1/2>)# apply mka policy MKA_Policy1
```

Removing MKA policy association from a port:

```
switch(config)# interface 1/1/1
switch(config-if)# no apply mka policy
```

Applying an MKA policy to a LAG port:

```
switch(config)# interface lag 1
switch(config-if)# apply mka policy MKA_Policy1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-if	Administrators or local user group members with execution rights for this command.

clear mka statistics

```
clear mka statistics [interface <IF-RANGE>]
```

Description

Clears MKA statistics on all MACsec-enabled interfaces or on a specific interface or interface range. MKA statistics are cleared for the entire switch rather than just in the current user session.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces (ports) for which MKA statistics information is to be cleared.

Examples

Clearing MKA statistics on an interface range:

```
switch# clear mka statistics interface 1/1/1-1/1/4
```

Clearing MKA statistics on all MACsec-enabled interfaces:

```
switch# clear mka statistics
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

data-delay-protection

```
data-delay-protection  
no data-delay-protection
```

Description

Configures the MACsec policy to use data delay protection. Data delay protection allows MKA participants to ensure that the data frames protected by MACsec are not delayed by more than 2 seconds.

Enabling data delay protection necessitates transmission of MKPDUs at a frequency of 0.5 second to meet a maximum data delay of 2 seconds while minimizing connectivity interruption due to the possibility of lost or delayed MKPDUs.

Data delay protection should be enabled only when there is a need to drop MACsec protected frames that are delayed by more than 2 seconds on the wire. It is recommended to not enable data delay protection unless absolutely required as it adds extra load on the system.

Disabled by default.



When data delay protection is enabled, a default of 0.5 second is used as transmit-interval and transmit-interval configuration under MKA policy is ignored.

Examples

Enabling data delay protection:

```
switch(config)# macsec policy Aggregator-Connect data-delay-protection
```

or

```
switch(config)# macsec policy Aggregator-Connect  
switch(config-macsec-policy)# data delay protection
```

Disabling data delay protection:

```
switch(config)# no macsec policy Aggregator-Connect data-delay-protection
```

or

```
switch(config)# macsec policy Aggregator-Connect  
switch(config-macsec-policy)# no data delay protection
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	config config-macsec-policy	Administrators or local user group members with execution rights for this command.

eapol-destination-mac

```
eapol-destination-mac <MAC-ADDRESS>  
no eapol-destination-mac <MAC-ADDRESS>
```

Description

Configures the destination MAC address to use in EAPoL frames for MKA. When not configured, the switch uses the default EAPoL multicast address (01:80:C2:00:00:03) for MKA.

The **no** form of the command configures the switch to use the default EAPoL multicast address for MKA.

MACsec WAN extension is only supported on the following switches:

Platform	SKU	Interfaces
9300S	S0F96A	1/1/1 - 1/1/8, 1/1/33 - 1/1/40

Parameter	Description
<MAC-ADDRESS>	Specifies the EAPoL destination MAC address for MKA.

Examples

Configuring the broadcast MAC as EAPoL destination address:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-destination-mac ff:ff:ff:ff:ff:ff
OR
switch(config)# mka policy Agg-To-Agg eapol-destination-mac ff:ff:ff:ff:ff:ff
```

Resetting MKA policy to use untagged EAPoL MKA frames:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# no eapol-destination-mac
OR
switch (config) # no mka policy Agg-to-Agg eapol-destination-mac
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	config-mka-policy	Administrators or local user group members with execution rights for this command.

eapol-dot1q-tagged

```
eapol-dot1q-tagged
no eapol-dot1q-tagged
```

Description

Configures the EAPoL frames for MKA to be transmitted with an 802.1q tag. The native VLAN associated with the port is used in the MKA frames. This configuration enables the switch to establish a MACsec tunnel over a Layer 2 network with the next hop connected over non-MACsec, 802.1q tagged only link. The **no** form of command configures the switch to send MKA frames as untagged.

MACsec WAN extension is only supported on the following switches:

Platform	SKU	Interfaces
9300S	S0F96A	1/1/1 - 1/1/8, 1/1/33 - 1/1/40



- When the configuration is enabled, MKA is restarted on the port if the native VLAN associated with the port is updated.
- The 802.1q tag added to the MKA frame is also used in the computation of the ICV for the MKA frame. If the 802.1q tag is removed or modified in any way along the path, including changes in VLAN ID or PCP, the MKA frame will be discarded at the destination.

Examples

Configuring the MKA policy to use 802.1q tagged EAPoL MKA frames:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-dot1q-tagged
OR
switch(config)# mka policy Agg-To-Agg eapol-dot1q-tagged
```

Resetting MKA policy to use untagged EAPoL MKA frames:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# no eapol-dot1q-tagged
OR
switch (config) # no mka policy Agg-to-Agg eapol-dot1q-tagged
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	config-mka-policy	Administrators or local user group members with execution rights for this command.

eapol-eth-type

```
eapol-eth-type <ETH-TYPE>
no eapol-eth-type <ETH-TYPE>
```

Description

Configures the Ether-Type for use in frames for MKA.

The **no** form of the command uses the default EAPoL ether-type 0x888e for MKA.

MACsec WAN extension is only supported on the following switches:

Platform	SKU	Interfaces
9300S	S0F96A	1/1/1 - 1/1/8, 1/1/33 - 1/1/40



- Only values 0x876f and 0x888e are supported.
- Refer to the MACsec WAN extension for a complete list of supported switch models.

Parameter	Description
<ETH-TYPE>	Configures the Ether-Type in EAPoL frames for MKA.

Examples

Configuring the custom Ethernet type for MKA:

```
switch(config)# mka policy Agg-To-Agg eapol-eth-type 876f
OR
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-eth-type 876f
```

Resetting the custom EAPoL Ethernet Type:

```
switch(config)# no mka policy Agg-To-Agg eapol-eth-type 876f
OR
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# no eapol-eth-type 876f
```

Using an Ethernet Type value other than 876f or 888e:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# eapol-eth-type 999F
Unsupported Ether-Type. Supported values are 888e and 876f
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	config-mka-policy	Administrators or local user group members with execution rights for this command.

key-server-priority

key-server-priority <PRIORITY>
no key-server-priority

Description

In the **config-mka-policy** policy context, configures the MKA key server priority. The highest priority is 0 and indicates that this switch strongly wants to be the MKA key server. The lowest priority is 255 and indicates that switch does not want to be the MKA key server, allowing the switch at the other end of the link to be the key server. Set this priority on the switches at either end of the link to achieve the desired effect.

If the key server priority is 0 on both switches then the switch with the lowest system MACsec address is elected as key server.

The **no** form of this command resets the MKA key server priority to its default of 0.

Parameter	Description
<PRIORITY>	Selects the MKA key server priority for this switch. Default 0 (highest priority). Range: 0 to 255.

Examples

Setting the MKA key server priority:

```
switch(config-mka-policy) # key-server-priority 5
```

Resetting the MKA key server priority to its default of 0:

```
switch(config-mka-policy) # no key-server-priority
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-mka-policy	Administrators or local user group members with execution rights for this command.

pre-shared-key

```
pre-shared-key keychain <NAME>
pre-shared-key ckn <CA-KEY-NAME> cak {plaintext [<PLAINTEXT-CAK>] | ciphertext
<CIPHERTEXT-CAK>}
```

Description

Configures the Pre-Shared Key (PSK) to use for an MKA policy.

A PSK can be configured one of two ways:

1. Configure the Connectivity Association Key Name (CKN) and Connectivity Association Key (CAK) directly in the PSK.
2. Configure the PSK to use an existing keychain for the CKN (key name) and CAK (key-string).

If both a key chain and a static CKN/CAK are configured in the PSK, then the key chain will be used for MKA operations.



When using a PSK with a key chain, only the send lifetime is considered for CAK lifetime. It is recommended to not configure an accept lifetime in the key chain used for MACsec.

The **no** form of this command deletes the PSK configuration including the key chain association, the CKN and the CAK.

Parameter	Description
<CA-KEY-NAME>	Specifies the CKN (Connectivity Association Key Name). Range: 1 to 64 hexadecimal characters.
<PLAINTEXT-CAK>	Specifies the CAK (Connectivity Association Key) in plaintext. Range: 1 to 64 hexadecimal characters.
<CIPHERTEXT-CAK>	Specifies the CAK (Connectivity Association Key) as ciphertext.
<NAME>	Specifies the keychain name.

Examples

Configuring the pre-shared key with a specified plaintext CAK:

```
switch(config-mka-policy) # pre-shared-key ckn abcdef12 cak plaintext 123abcdef
```

Configuring the pre-shared key with a prompted plaintext CAK:

```
switch(config-mka-policy) # pre-shared-key ckn abcdef12 cak plaintext
Enter CAK: *****
Confirm CAK: *****
```

Configuring the pre-shared key with a ciphertext CAK:

```
switch(config-mka-policy) # pre-shared-key ckn abcdef12 cak ciphertext
AQBapUvjDZgUxtTpgA4NLqnsn7CjXqbDch+BOS7y9fcWExLUBgAAAKUmDYdhew==
```

Configuring a key chain for an MKA policy:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# pre-shared-key keychain macsec_keys
```

Deleting the PSK configuration including its CKN and CAK:

```
switch(config-mka-policy)# no pre-shared-key
```

Deleting a key chain from an MKA policy:

```
switch(config)# mka policy Agg-To-Agg
switch(config-mka-policy)# no pre-shared-key keychain macsec_keys
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	config-mka-policy	Administrators or local user group members with execution rights for this command.

mka policy

```
mka policy <MKA-POLICY-NAME>
no mka policy <MKA-POLICY-NAME>
```

Description

Creates the specified MKA (MACsec Key Agreement) policy and then enters its context (displayed in the CLI as **config-mka-policy**). If the MKA policy already exists, this command enters the specified MKA policy context.

An MKA policy can be applied to one or more switch ports, enabling MKA on the ports. A MACsec policy must be applied to the same ports.

The **no** form of this command deletes the MKA policy.



An MKA policy cannot be deleted if it is currently applied to any ports. All application of the policy must be removed before the policy can be deleted.

Parameter	Description
<code><MKA-POLICY-NAME></code>	Specifies the MKA policy name. Range: 1 to 32 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Creating an MKA policy:

```
switch(config)# mka policy MKA_Policy1
switch(config-mka-policy)#
```

Deleting an MKA policy (policy cannot be deleted if the mka policy is currently applied to any ports):

```
switch(config)# no mka policy MKA_Policy1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	config	Administrators or local user group members with execution rights for this command.

show mka policy

`show mka policy [<MKA-POLICY-NAME>]`

Description

Shows information for one or all MKA policies.

Parameter	Description
<code><MKA-POLICY-NAME></code>	Specifies the MKA policy name. Range: 1 to 32 alphanumeric characters including only the three special characters "." (period), "-" (hyphen), and "_" (underscore).

Examples

Showing information for a specific MKA policy:

```
switch(config)# show mka policy mka1
```

```
MKA Policy Details
=====
```

```
Policy Name: mka1
```

```
-----
Mode                : Pre-shared key
CKN                 : 123
CAK (encrypted)     : AQBapdmm17Ql4DWgACmS0iX7JrkVUvfRg4NvDvuQm6+...
Keychain            :
EAPoL Destination MAC : 01:80:c2:00:00:03
EAPoL Ethernet Type  : 888e
EAPoL 802.1q Tag     : Disabled
Key-server Priority   : 0
Transmit Interval    : 2 seconds
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mka statistics

```
show mka statistics [interface <IF-RANGE>]
```

Description

Shows MKA statistics for all MACsec-enabled interfaces or a specific interface or interface range. The MKA statistics are refreshed periodically, approximately every five seconds.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MKA statistics information is to be shown.

Examples

Showing MKA statistics information for a specific interface:


```
switch# show mka statistics interface 1/1/1
```

```
Interface 1/1/1
=====
```

```
KaY
```

```
----
```

```
SCI : ec0273f72f4d0001
```

```
Statistics
```

```
-----
```

```
MKPDUs With Invalid Version : 0
```

```
MKPDUs With Invalid CKN      : 0
```

```
Participant
```

```
-----
```

```
CKN : 1234567890
```

```
Statistics
```

```
-----
```

```
Tx MKPDUs                : 33834
```

```
Rx MKPDUs                : 35375
```

```
SAKs Distributed         : 1
```

```
SAKs Received            : 0
```

```
MKPDUs With Invalid ICV  : 0
```

```
MKPDUs With Duplicate MI : 0
```

```
MKPDUs With Invalid MN   : 0
```

```
...
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mka status

```
show mka status [interface <IF-RANGE>]
```

Description

Shows MKA status information for all MACsec-enabled interfaces or a specific interface or interface range.

Parameter	Description
interface <IF-RANGE>	Specifies one or more interfaces for which MKA status information is to be shown.

Examples

Showing MKA status information for a specific interface (Pre-shared key):

```
switch(config)# show mka status

MKA Protocol Status

Interface 1/1/4
=====

MKA Port Identifier      : 1
MKA Policy Name         : mka1
MKA Session Status      : Unsecured
Mode                    : Pre-shared key
CKN                     : 1230
CAK (encrypted)         :
AQBapTPSRl29UzarAbF0NrxgsU3B8Z5w9lhEz/oKjWMbf7+6AwAAAMMlEQ==
Keychain                :
Member Identifier       : f84f8bd77971b527c4a7e370
Message Number          : 2
Capability               : IC, Conf, Offset 0
EAPoL Destination MAC   : 01:80:c2:00:00:03
EAPoL Ethernet Type     : 888e
EAPoL 802.1q Tagged     : Disabled
Transmit Interval       : 2 seconds
Key Server Priority      : 0
Key Server              : Yes
Live Peer List:
MI                      MN      PRI Capability      Rx-SCI
-----
Potential Peer List:
MI                      MN      PRI Capability      Rx-SCI
-----
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S Switch Series.

Command Information

Platforms	Command context	Authority
9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

transmit-interval

```
transmit-interval <INTERVAL>
no transmit-interval
```

Description

In the **config-mka-policy** policy context, configures the MKA packet transmit interval.
The **no** form of this command resets the MKA packet transmit interval to its default of 2 seconds.

Parameter	Description
<INTERVAL>	Selects the MKA packet transmit interval. Default 2 seconds. Range: 2 to 6 seconds.

Examples

Setting the MKA packet transmit interval:

```
switch(config-mka-policy) # transmit-interval 4
```

Resetting the MKA packet transmit interval to its default of 2 seconds:

```
switch(config-mka-policy) # no transmit-interval
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300S.

Command Information

Platforms	Command context	Authority
9300S	config-mka-policy	Administrators or local user group members with execution rights for this command.

MLD snooping global configuration

ipv6 mld snooping

```
ipv6 mld snooping drop-unknown {vlan-shared | vlan-exclusive}  
no ipv6 mld snooping drop-unknown {vlan-shared | vlan-exclusive}
```

Description

This command configures the drop unknown mode. While MLD snooping is enabled, the traffic will be forwarded only to ports that initiate an MLD request for multicast. Drop unknown mode can be a filter across all VLANs (vlan-shared) or per VLAN (exclusive-vlan). The default configuration is vlan-shared.

The **no** form of this command configures the drop unknown mode on the switch to the default **vlan-shared**.

Parameter	Description
vlan-shared	Required: Enable shared VLAN filter on the switch.
vlan-exclusive	Required: Enable exclusive drop unknown filter per VLAN.

Example

```
switch(config)# ipv6 mld snooping drop-unknown vlan-shared  
switch(config)# ipv6 mld snooping drop-unknown vlan-exclusive  
switch(config)# no ipv6 mld snooping drop-unknown
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config	Administrators or local user group members with execution rights for this command.

MLD snooping VLAN configuration

ipv6 mld snooping

```
ipv6 mld snooping {enable | disable}  
no ipv6 mld snooping [enable | disable]
```

Description

This command disables or reenables MLD snooping on the VLAN. Starting with AOS-CX 10.16, MLD snooping is enabled by default.

The **no** form of this command disables all MLD snooping configurations on the VLAN.

Parameter	Description
enable	Reenable MLD snooping on the VLAN.
disable	Disable MLD snooping on the VLAN.

Example

Disable and then reenables MLD snooping on VLAN 2:

```
switch(config)# vlan 2  
switch(config-vlan)# ipv6 mld snooping disable  
switch(config-vlan)# ipv6 mld snooping enable
```

Remove all MLD snooping configurations on VLAN 2:

```
switch(config)# vlan 2  
switch(config-vlan)# no ipv6 mld snooping enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.16	Starting with this release, MLD snooping is enabled on VLANs by default, including the Management VLAN (vlan 1) and VLANs with a associated VNI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	<code>config-vlan-<VLAN-ID></code>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping apply access-list

```
ipv6 mld snooping apply access-list <ACL-NAME>
no ipv6 mld snooping apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command disables the rules set for the ACL.



This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameter	Description
<code>access-list</code>	Associates an ACL with the IGMP.
<code><ACL-NAME></code>	Specifies the name of the ACL. NOTE: If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
```

```
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld snooping apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list `mygroup`:

```
switch(config-vlan)# no ipv6 mld snooping apply access-list mygroup
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping all-vlans

```
ipv6 mld snooping all-vlans
no ipv6 mld snooping all-vlans
```

Description

Enable MLD snooping on all VLANs. This configuration setting enables MLD snooping on all existing VLANs, as well as on any VLANs that are created after the **ipv6 mld snooping all-vlans** command is issued. When MLD snooping is enabled globally, MLD snooping can not be configured on individual VLANs within the VLAN context of the command-line interface.

The **no** form of this command disables global MLD snooping, allows MLD snooping to remain enabled at the VLAN level, and allows the configuration of VLAN-level MLD snooping settings.

Example

Configure MLD snooping globally:

```
switch(config)# ipv6 mld snooping all-vlans
```

Disable global IGMP snooping:

```
switch(config)# no ipv6 mldsnoping all-vlans
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

Release	Modification
10.16	Command introduced

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	<code>config</code>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping auto vlan

```
ipv6 mld snooping [auto vlan <VLAN-LIST>]  
no ipv6 mld snooping [auto vlan <VLAN-LIST>]
```

Description

This command configures the given ports in auto mode, which is the default port mode. The **no** form of this command disables auto ports.

Parameter	Description
<code><VLAN-LIST></code>	Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring auto ports for VLANs on the interface:


```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping auto vlan 10
switch(config-vlan)# ipv6 mld snooping auto vlan 10-20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping blocked vlan

```
ipv6 mld snooping [blocked vlan <VLAN-LIST>]
no ipv6 mld snooping [blocked vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in blocked mode.

The **no** form of this command removes blocked ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a blocked port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring blocked ports for the VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping blocked vlan 10
```

```
switch(config-vlan)# ipv6 mld snooping blocked vlan 10-20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastlearn

```
ipv6 mld snooping fastlearn <port-list>
```

Description

This command enables the port to learn group information on receiving topology change notification. The **no** form of this command disables fastlearn on the ports.

Parameter	Description
port-list	Required: 1/1/1-1/1/2, ports to be configured as fastlearn ports.

Example

```
switch(config)# ipv6 mld snooping fastlearn 1/1/3
switch(config)# ipv6 mld snooping fastlearn 1/1/1-1/1/2
switch(config)# ipv6 mld snooping fastlearn 1/1/5,1/1/6
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastleave vlan

```
ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
no ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
```

Description

Configures the specified ports as fastleave ports. Enables the switch to immediately remove an interface from the bridge table upon receiving the leave group message.

The **no** form of this command disables fastleave configuration on the ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

MLD fastleave is configured for ports on a per-VLAN basis. By default, the querier sends a MLD Group-Specific Query message out of the interface, upon which the leave group message is received to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host. Fastleave processing eliminates the MLD Group-Specific Query message. Thus, it allows the switch to immediately remove an interface from the bridge table upon receiving the leave Group message. This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an MLD Group-Specific Query message.

Example

Configuring fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10-20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forced fastleave vlan

```
ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
no ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
```

Description

Configures the given ports in forced fastleave mode.

The **no** form of this command disables forced fastleave configuration on the ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a forced fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

With forced fastleave enabled, MLD speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits a small amount of time to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port.

Example

Configuring forced-fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10-20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forward vlan

```
ipv6 mld snooping [forward vlan <VLAN-LIST>]
no ipv6 mld snooping [forward vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in forward mode.

The **no** form of this command disables forward ports.

Parameter	Description
<VLAN-LIST>	Required: Specifies a list of VLANs on which the port should be configured as a forward port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

Configuring forward ports for VLANs on the interface:

```
switch# configureterminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forward vlan 10
switch(config-vlan)# ipv6 mld snooping forward vlan 10-20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping querier-address

```
ipv6 mld snooping querier-address <QUERIER-IP-ADDRESS>
no ipv6 mld snooping querier-address <QUERIER-IP-ADDRESS>
```

Description

Configures the MLD querier IPv6 address for the IGMP-MLD proxy feature in EVPN. The **no** form of this command removes the configuration.

Parameter	Description
<QUERIER-IP-ADDRESS>	Specifies the proxy querier IPv6 address.

Usage

This command is used in conjunction with the IGMP-MLD proxy feature of EVPN.



This is an optional command applicable to VTEPs that have Layer 2 VLANs (without an IPv6 address) and require IGMP-MLD proxy querier functionality.

If a Layer 3 SVI with an IPv6 address is configured for the VLAN, it takes precedence. In the absence of a valid IPv6 address or SVI, the given IP address is used for querier operations.

This configuration is global and applies to all tenants' Layer 2 VLANs where the IGMP-MLD proxy feature is enabled.

Fabrics running the **igmp-mld proxy** feature must perform distributed querier functionality on every VTEP where the VLAN is extended. This configuration is applicable only when **igmp-mld-proxy** configuration is configured under EVPN.

In the event of underlay tunnel fluctuations, the querier state reinitializes and transitions back to the querier state only after the default querier wait of 260 seconds.

This configuration is not applicable to VLANs that are not mapped to a VNI.



The specified IP address does not need to be assigned to any interface.

Example

Configures the MLD querier IPv6 address for the IGMP-MLD proxy feature in EVPN.

```
switch(config)# ipv6 mld snooping querier-address fe80::2002
```

Remove the configuration of the MLD querier IPv6 address for the IGMP-MLD proxy feature in EVPN.

```
switch(config)# no ipv6 mld snooping querier-address fe80::2002
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.16	Command introduced

Command Information

Platforms	Command context	Authority
All platforms,	config	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping static-group

```
ipv6 mld snooping [static-group <X:X::X:X>]  
no ipv6 mld snooping [static-group <X:X::X:X>]
```

Description

This command configures static multicast group.

The **no** form of this command disables static multicast group.

Parameter	Description
static-group	Required: <X:X::X:X>, MLD static multicast group.

Example

Configuring static multicast group:

```
switch(config)# vlan 2  
switch(config-vlan)# ipv6 mld snooping static-group ff12::c
```

Removing the configuration of static multicast group:

```
switch(config)# vlan 2  
switch(config-vlan)# no ipv6 mld snooping static-group ff12::c
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan- <i><VLAN-ID></i>	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping version

```
ipv6 mld snooping [version <ver>]
no ipv6 mld snooping [version <ver>]
```

Description

This command configures the MLD snooping version on the VLAN. MLD version 2 is the default. The **no** form of the command configures the default MLD snooping version on the VLAN, **2**.

Parameter	Description
ver	Required: 1-2, MLD snooping version.

Example

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping version 2
```

```
switch(config-vlan)# no ipv6 mld snooping version 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms,	config-vlan- <i><VLAN-ID></i>	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
except for S3L75A, S3L76A, S3L77A		

MLD snooping show commands

show ipv6 mld snooping

```
show ipv6 mld snooping [vlan <vlan-id> [group <ip-addr>|{port <IF-NAME>}|{vsx-peer}]
  counters
  detail
  groups [vlan <vlan-id> [vsx-peer [vlan <vlan-id>]]
  no ...
  packet-exceptions
  static-groups [vsx-peer]
  statistics
  vsx-peer vlan [<vlan-id>]
```

Description

This command shows MLD snooping details for all VLANs. Specify a VLAN ID or a VLAN and a group to display details for only that VLAN or VLAN group.

Parameter	Description
vlan <vlan-id>	Shows MLD snooping protocol information and number of different groups joined for the VLAN.
group	Shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN. Identify the group by IP address or interface name.
<ip-addr>	Display MLD snooping information for the selected group IP address.
port <IF-NAME>	Display information for a VLAN port. Specify the port name in member/slot/port format.
vsx-peer	Display VSX peer switch information.
counters	Shows MLD query packets transmitted (Tx), received (Rx), and error packet counters.
detail	Shows the total VLANs with MLD enabled. When issued with the vlan <vlan-id> parameter, this command displays details for the selected VLAN.
groups	Show MLD snooping groups information.
vlan <vlan-id>	Display IGMP snooping operational information for specified VLAN
[vsx-peer [vlan <vlan-id>]]	Display IGMP snooping operational information for the specified vsx-peer switch.

Parameter	Description
no ...	Negates any configured parameter.
packet-exceptions	Troubleshoot issues in an L2 multicast bridge entries for data packets forwarded to the CPU.
static-groups [vsx-peer]	Shows MLD snooping static group details, including the number of static groups joined. Include the optional [vsx-peer] parameter to display VSX peer switch information.
statistics	Show MLD snooping statistics.
[vsx-peer] vlan <vlan-id>	Displays VSX peer switch information for the specified VLAN ID.

Examples

```
switch# show ipv mld snooping vlan 2 group port 1/1/1
```

```
VLAN ID   : 2
VLAN Name : VLAN2
```

```
Group Address : ff05::2:1
Last Reporter  : fe80::1
Group Type     : Filter
```

Port	Vers	Mode	Uptime	Expires	Vl Timer	Sources Forwarded	Sources Blocked
1/1/1	2	INC	1m 46s	2m 34s		3	0

```
Group Address : ff05::2:1
Source Address : 3000::1
Source Type    : Filter
```

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

```
Group Address : ff05::2:1
Source Address : 3000::2
Source Type    : Filter
```

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

```
Group Address : ff05::2:1
Source Address : 3000::3
Source Type    : Filter
```

Port	Mode	Uptime	Expires	Configured Mode
1/1/1	INC	1m 46s	2m 34s	Auto

```
switch# show ipv6 mld snooping counters
```

```
MLD Snooping VLAN Counters
```

```
Rx Counters :
```

```

V1 All Hosts Queries          0
V2 All Hosts Queries          0
V2 Group Specific Queries     0
Group And Source Specific Queries 0
V1 Member Reports             0
V2 Member Reports             0
V1 Member Leaves              0

```

Tx Counters :

```

Flood on vlan                 44
V1 Group Specific Queries     0
V2 Group Specific Queries     0

```

Errors:

```

Unknown Message Type          0
Malformed Packets             0
Bad Checksum                   0
Packet received on MLD-disabled Interface 0
Interface Wrong Version Queries 0
Packets dropped by ACL         0

```

Port Counters:

```

Membership Timeout            0

```

switch# show ipv6 mld snooping groups

MLD Group Address Information

VLAN ID	Group Address	Expires	UpTime	Last Reporter	Type
10	ff12::c	3m 54s	0m 26s	2001::1	
Filter					
10	ff12::d	4m 17s	0m 3s	2001::1	

switch# show ipv6 mld snooping vlan 2 statistics

MLD Snooping statistics

```

VLAN ID      : 2
VLAN Name    : VLAN2

```

```

Number of Include Groups      : 1
Number of Exclude Groups      : 0
Number of Static Groups       : 1
Total Multicast Groups Joined : 2

```

switch# show ipv6 mld snooping packet-exceptions

List of L2 Multicast Bridge entries for which data packets are hitting CPU

Vlan	Group Address	Source-Address	Packet Count	Last Seen Time
10	ff03::10/128	1010::10/128	19	01h:02m:05s
10	ff03::12/128	1010::11/128	30	00d:02h:01m
10	ff04::10/12	1010::10/128	40	01m:02w:03d
20	ff03::11/128	5000::10/128	20	02m:02w:00d

20	ff03::12/128	5000::10/128	41	0001y:01m:02w:05d
20	ff04::10/128	5000::10/128	30	00d:02h:02m



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	The packet-exceptions parameter is introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mgmd debug-counters

show mgmd debug-counters

Description

This command displays packet throttle counters and packet queue sizes for IGMP/MLD debug counters.

Example

```
switch# show mgmd debug-counters
Global MGMD Debug Counters
Group Throttle Count                : 0
Dropped Packet Count                : 100
Max Pkt Handler Queue Depth        : 2048
Current Pkt Handler Queue Depth    : 1000
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	<code>config</code>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 mld

```
ipv6 mld {enable | disable}  
no ipv6 mld [enable | disable]
```

Description

This command enables or disables MLD on the interface VLAN.

The **no** form of this command disables MLD on the interface VLAN.

Parameter	Description
enable	Required: Enable MLD on the interface VLAN.
disable	Required: Disable MLD on the interface VLAN.

Example

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ipv6 mld enable  
switch(config-if-vlan)# ipv6 mld disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list

```
ipv6 mld apply access-list <ACL-NAME>
```

```
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command disables the rules set for the ACL.

Parameter	Description
<code>access-list</code>	Associates an ACL with the IGMP.
<code><ACL-NAME></code>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

no ipv6 mld

no ipv6 mld

Description

This command removes all MLD configurations on the interface.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 mld
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier

ipv6 mld querier

Description

This command configures MLD querier.

The **no** form of this command disables MLD querier.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier
switch(config-if-vlan)# no ipv6 mld querier
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval

```
ipv6 mld querier [interval <interval-value>]
```

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameter	Description
interval-value	Required: 5-300, configures MLD querier interval. NOTE: Default interval-value is 125. Use the no ipv6 mld querier interval command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier interval 100
switch(config-if-vlan)# no ipv6 mld querier interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier-wait-time

```
ipv6 mld querier-wait-time <QUERIER-WAIT-TIME>
[no] ipv6 mld querier-wait-time <QUERIER-WAIT-TIME>
```

Description

Configures initial MLD querier-wait-time value in seconds.

The **no** form of this command sets the MLD querier-wait-time to the default value of 260 seconds. Note that the wait timer can be configured to any numbers within the 1-300 second range.

Parameter	Description
<QUERIER-WAIT-TIME-VALUE>	Configures MLD querier-wait-time to desired value.

Example

```
switch (config-if-vlan) # ipv6 mld querier-wait-time
<1-300> Querier Wait value (Default: 260)
switch (config-if-vlan) #
```



When PIMv6 is enabled, automated election will override querier-wait-time configuration. When PIM is disabled and **[no] igmp querier-wait-time** is configured, the initial wait timer will be configured at desired value.

For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms,	config-if-vlan	Administrators or local user group members with execution

Platforms	Command context	Authority
except for S3L75A, S3L76A, S3L77A		rights for this command.

ipv6 mld last-member-query-interval

ipv6 mld last-member-query-interval <interval-value>

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameter	Description
interval-value	Required: 1-2, configures MLD last-member-query-interval.



Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld last-member-query-interval 2
switch(config-if-vlan)# no ipv6 mld last-member-query-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time

ipv6 mld querier query-max-response-time <response-time>

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameter	Description
max-response-time-value	Required: 10-128, configures MLD querier max-response-time. NOTE: Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld query-max-response-time 50
switch(config-if-vlan)# no ipv6 mld query-max-response-time
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness

ipv6 mld robustness <VALUE>

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameter	Description
<VALUE>	Required: 1-7, configures MLD robustness.

Parameter	Description
	NOTE: Default robustness-value is 2 seconds. Use the no ipv6 mld robustness command to set robustness-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld robustness 5
switch(config-if-vlan)# no ipv6 mld robustness
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group

ipv6 mld static-group <MULTICAST-GROUP-IP>

Description

This command configures MLD static group.

Parameter	Description
<MULTICAST-GROUP-IP>	Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld static-group ff12::c
switch(config-if-vlan)# no ipv6 mld static-group ff12::c
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld version

```
ipv6 mld version <VERSION>  
no ipv6 mld version <VERSION>
```

Description

This command configures MLD version.

The **no** form of the command configures the default MLD version of **2**.

Parameter	Description
<VERSION>	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2  
switch(config-if-vlan)# ipv6 mld version 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A,	config-if-vlan	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
S3L76A, S3L77A		

ipv6 mld version strict

ipv6 mld version <VERSION> [strict]

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameter	Description
<VERSION>	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2 strict
switch(config-if-vlan)# no ipv6 mld version 2 strict
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if-vlan	Administrators or local user group members with execution rights for this command.

MLD show commands for interface VLAN

show ipv6 mld

```
show ipv6 mld
  all-vrfs
  counters
  group <x:x::x:x> [source x:x::x:x]
  groups
  interface {<INTF-ID>|<INTF-ID.ID>}|{vlan <vlan-id>}}
  static-groups
  statistics [all-vrfs|{vrf <vrf-name>}]
  vrf <vrf-name>
  vsx-peer
```

Description

This command shows MLD groups joined details.

Parameter	Description
all-vrfs	Show MLD snooping info for all VRFs in all interfaces or groups, or for all VRFs in a specified group, interface or VLAN
counters	Show all MLD counters, or display counters for the specified interface or VLAN
group <x:x::x:x> [source <x:x::x:x>]	Show MLD group information for the specified group, group and interface, or group and vlan. Include the optional source <x:x::x:x> parameter to display source information for the group.
groups	Show MLD group information for all VRFs, or for groups in the specified interface or VLAN.
interface	Shows MLD configuration information for a specified interface or VLAN.
<INTF-ID>	Specify an Interface ID
	Specify a sub-interface ID. (Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.)
vlan <vlan-id>	Specify a VLAN ID
static-groups	Display all static groups information, or include one of the additional parameters apply additional filters: ▪ all-vrfs: Display MLD static-group information for all VRFs ▪ vrf <vrf-name>: Display MLD static-group information

Parameter	Description
	for the selected VRF
statistics	Display all MLD statistics, or include one of the additional parameters apply additional filters: ▪ all-vrfs: Display MLD statistics information for all VRFs ▪ vrf <vrf-name>: Display MLD statistics information for the selected VRF
vrf <vrf-name>	Show MLD information for the specified VRF.
vsx-peer	Display VSX-peer information.

Examples

Showing the current MLD configuration and status

```
switch# show ipv6 mld

VRF Name           : default
Interface          : vlan10
MLD Configured Version : 2
MLD Operating Version : 2
Querier State      : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime     : 39m 44s
Querier Expiration Time : 0m 31s
MLD Snoop Enabled on VLAN : True
```

Showing the MLD configuration on a specified VLAN or interface:

```
switch# show ipv6 mld interface vlan 10

MLD Configured Version : 2
MLD Operating Version : 2
Querier State      : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime     : 40m 42s
Querier Expiration Time : 1m 39s
MLD Snoop Enabled on VLAN : True

switch# show ipv6 mld interface 1/1/2

MLD Configured Version : 2
MLD Operating Version : 2
Querier State      : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:d3ec
Querier Uptime     : 40m 42s
Querier Expiration Time : 1m 39s
MLD Snoop Enabled on VLAN : True
```

Showing MLD configuration on sub-interface 1/1/2.10:



Applies only to the HPE Aruba Networking 6300, 6400, 8100, 8325/8325H/8325P, 8360, 9300, 9300S, and 10000 Switch Series.

```
switch# show ipv6 mld interface 1/1/2.10

MLD Configured Version   : 2
MLD Operating Version    : 2
Querier State            : Querier
Querier IP [this switch] : fe80::7272:cfff:fe96:13ec
Querier Uptime           : 40m 42s
Querier Expiration Time  : 1m 39s
MLD Snoop Enabled on VLAN : True
```

Showing MLD groups information for a specified interface:

```
switch# show ipv6 mld interface 1/1/1 groups

MLD group information for group ff55::1

Interface Name   : 1/1/1
VRF Name         : default

Group Address    : ff55::1
Last Reporter    : fe80::a00:9ff:fe77:1062

Vers  Mode  Uptime    Expires    V1          Sources    Sources
-----
2     EXC    0m 14s      4m 6s      Timer       Forwarded  Blocked
```

Showing MLD groups information for a specified sub-interface:

```
switch# show ipv6 mld interface 1/1/1.10 groups

MLD group information for group ff56::1

Interface Name   : 1/1/1.10
VRF Name         : default

Group Address    : ff56::1
Last Reporter    : fe80::a00:9ff:fe77:1062

Vers  Mode  Uptime    Expires    V1          Sources    Sources
-----
2     EXC    1m 14s    2m 6s      Timer       Forwarded  Blocked
```

Showing MLD static groups

```
switch# show ipv6 mld static-groups all-vrfs

MLD Static Group Address Information

VRF Name :default
Interface Name  Group Address
-----
vlan2          ff12::c
vlan2          ff12::d
VRF Name :test
Interface Name  Group Address
```

```

-----
vlan3          ff13::1
vlan3          ff13::2

```

Showing MLD counters

```
switch# show ipv6 mld counters
```

MLD Counters

```
Interface Name      : vlan2
VRF Name            : default
Membership Timeout   : 0
```

	Rx	Tx
	-----	-----
V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	12
V1 Group Specific Queries	0	0
V2 Group Specific Queries	0	0
Group And Source Specific Queries	0	0
V2 Member Reports	0	N/A
V1 Member Reports	0	N/A
V1 Member Leaves	0	N/A
Packets dropped by ACL	0	N/A

```
switch# show ipv6 mld counters vrf default
```

MLD Counters

```
Interface Name      : vlan2
VRF Name            : default
Membership Timeout   : 0
```

	Rx	Tx
	-----	-----
V1 All Hosts Queries	0	0
V2 All Hosts Queries	0	12
V1 Group Specific Queries	0	0
V2 Group Specific Queries	0	0
Group And Source Specific Queries	0	0
V2 Member Reports	0	N/A
V1 Member Reports	0	N/A
V1 Member Leaves	0	N/A
Packets dropped by ACL		

Showing MLD statistics on a specified interface:

```
switch# show ipv6 mld interface 1/1/1 statistics
```

MLD statistics

```
Interface Name : 1/1/1
VRF Name       : default
```

```
Number of Include Groups      : 2
Number of Exclude Groups     : 0
Number of Static Groups       : 0
Total Multicast Groups Joined : 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.17	Sub-interface support extended to 9300 and 9300S Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 mld

```
ipv6 mld {enable | disable}  
no ipv6 mld {enable | disable}
```

Description

This command enables or disables MLD on the interface.

The **no** form of this command disables MLD on the interface.

Parameter	Description
enable	Required: Enable MLD on the interface.
disable	Required: Disable MLD on the interface.

Example

```
switch(config)# interface 1/1/1  
switch(config-if)# ipv6 mld enable  
switch(config-if)# ipv6 mld disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list

```
ipv6 mld apply access-list <ACL-NAME>
```

```
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The **no** form of this command removes the rules set for the ACL.

Parameter	Description
access-list	Associates an ACL with the IGMP.
<ACL-NAME>	Specifies the name of the ACL.

Usage

- Existing classifier commands are used to configure the ACL.
- In case an IGMPv3 packet with multiple group addresses is received, the switch only processes the permitted group addresses based on the ACL rule set. The packet is forwarded to querier and PIM router even though one of the groups present in the packet is blocked by ACL. This avoids the delay in learning of the permitted groups. Since the access switch configured with ACL blocks the traffic for the groups which are denied, forwarding of joins has no impact. If all the groups in the packet are denied by the ACL rule, the packet is not forwarded to the querier and PIM router. Existing joins will timeout.
- In case of IGMPv2, if there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on permit/deny rules set in access list **mygroup**:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# 10 deny icmpv6 any ff55::2
switch(config-acl-ip)# 20 deny icmpv6 any ff55::3
switch(config-acl-ip)# 30 permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface 1/1/1
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list **mygroup**:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-vlan	Administrators or local user group members with execution rights for this command.

no ipv6 mld

no ipv6 mld

Description

This command removes all MLD configurations on the interface.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 mld
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier

ipv6 mld querier

Description

This command configures MLD querier. This functionality will allow the interface to join in the querier-election process.

Example


```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld querier
switch(config-if)# no ipv6 mld querier
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval

```
ipv6 mld querier [interval <interval-value>]
```

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameter	Description
interval-value	Required: 5-300, configures MLD querier interval. NOTE: Default interval-value is 125. Use the <code>no ipv6 mld querier interval</code> command to set interval-value to the default.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld querier interval 100
switch(config-if)# no ipv6 mld querier interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval

ipv6 mld last-member-query-interval <interval-value>

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameter	Description
interval-value	Required: 1-2, configures MLD last-member-query-interval.



Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld last-member-query-interval 2
switch(config-if)# no ipv6 mld last-member-query-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time

ipv6 mld querier query-max-response-time <response-time>

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameter	Description
max-response-time-value	Required: 10-128, configures MLD querier max-response-time. NOTE: Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld querier query-max-response-time 50
switch(config-if)# no ipv6 mld querier query-max-response-time
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness

ipv6 mld robustness <value>

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameter	Description
robustness-value	Required: 1-7, configures MLD robustness.



Default robustness-value is 2 seconds. Use the `no ipv6 mld robustness` command to set robustness-value to the default.

Example

```
switch(config)# interface 1/11/1
switch(config-if)# ipv6 mld robustness 5
switch(config-if)# no ipv6 mld robustness
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group

ipv6 mld static-group <multicast-group-ip>

Description

This command configures MLD static group.

Parameter	Description
multicast-group-ip	Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld static-group ff12::c
switch(config-if)# no ipv6 mld static-group ff12::c
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version

```
ipv6 mld version <version>
no ipv6 mld version <version>
```

Description

This command configures MLD version.

The **no** form of this command removes MLD version from the interface.

Parameter	Description
version	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld version 2
```

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 mld version 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict

ipv6 mld version <version> [strict]

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameter	Description
version	Required: 1-2, configures MLD version.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld version 2 strict
switch(config-if)# no ipv6 mld version 2 strict
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms, except for S3L75A, S3L76A, S3L77A	config-if	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables MSDP on the VRF.

Example

Disabling MSDP:

```
switch(config)# router mdp
switch(config-msdp)# disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables MSDP on the VRF.

Example

Enabling MSDP:

```
switch(config)# router msdp
switch(config-msdp)# enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp	Administrators or local user group members with execution rights for this command.

router msdp

```
router msdp [vrf <VRF-NAME>]
no router msdp [vrf <VRF-NAME>]
```

Description

Changes the current context to the MSDP router context. If no VRF is specified, the default VRF MSDP context of the router is assumed.

The **no** form of this command removes the MSDP configuration from the specified context or the default VRF.

Parameter	Description
vrf <VRF-NAME>	Specifies the context to the specified VRF.

Examples

Configuring default MSDP router context:

```
switch(config)# router msdp
switch(config-msdp)#
```

Configuring specified router MSDP:

```
switch(config-msdp)# router msdp vrf red
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

sa-interval

```
sa-interval <INTERVAL-VALUE>
no sa-interval
```

Description

Configures the sa-interval for the frequency at which MSDP source-active messages are sent. The **no** form of this command sets the interval to the default value of 60 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the sa-interval in seconds. Default: 60 seconds. Range 60-65535.

Examples

Configuring the sa-interval:

```
switch(config)# router mdp
switch(config-mdp)# sa-interval 400
switch(config-mdp)# no sa-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-mdp	Administrators or local user group members with execution rights for this command.

sa-limit

```
sa-limit <LIMIT-VALUE>
no sa-limit <LIMIT-VALUE>
```

Description

Configures the SA (Source Active) cache limit for the MSDP peer.
The **no** form of this command sets the cache limit to the default value.

Parameter	Description
<LIMIT-VALUE>	Specifies the sa cache limit. MSDP peer limit: 64, Cache Limit: 8K

Usage

This command is used to limit the overall number of (S, G) entries that a device can accept from specified MSDP peers and store in a sa-cache. When configured, the device maintains a per-peer count of (S, G) messages stored in the SA cache and ignores new messages from a peer if the configured sa-limit for that peer has been reached. This command protects MSDP-enabled devices from denial of service (DOS) attacks.

By default, there is no limit configured per peer. All (S, G) entries within the system capacities are allowed. If there is a reboot or HA switchover, the (S, G) cache allocation occurs based on FCFS basis. When configured via CLI or REST, (S, G) entries are allocated until they reach the system capacity or peer limit based on whichever is reached first and new sets of (S, G) requests are discarded.

Examples

Configuring the sa cache limit to 1000:

```
switch(config)# router mdp
switch(config-mdp)# ip mdp peer 10.1.1.1
switch(config-mdp-peer)#
switch(config-mdp-peer)# sa-limit 1000
```

Removing the configured sa cache limit of 1000:

```
switch(config)# router mdp
switch(config-mdp)# ip mdp peer 10.1.1.1
switch(config-mdp-peer)#
switch(config-mdp-peer)# no sa-limit 1000
```

Configuring the sa cache limit outside system capacities:

```
switch(config)# router mdp
switch(config-mdp)# ip mdp peer 10.1.1.1
switch(config-mdp-peer)#
switch(config-mdp-peer)# sa-limit 20000
Specified value exceeds the system capacities. Maximum SA Allowed on the system is 16384.
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-msdp</code>	Administrators or local user group members with execution rights for this command.

MSDP peer configuration commands

connection-retry-interval

```
connection-retry-interval <INTERVAL-VALUE>
no connection-retry-interval
```

Description

Configures the connection-retry-interval for which MSDP peers will wait after peering sessions are reset, before attempting to re-establish the peering sessions.

The **no** form of this command removes the currently configured value and sets it to the default value of 30 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specify connection-retry-interval in seconds. Range: 1-65535.

Example

Configuring the connection-retry-interval:

```
switch(config-msdp-peer) # connection-retry-interval 120
switch(config-msdp-peer) # no connection-retry-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

connect-source

```
connect-source <INTERFACE-NAME>
```

Description

Configures the connection source interface for the MSDP Peer.

The **no** form of this command removes the existing connection source interface and resets the peer connection.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the interface to use as a source.

Examples

Configuring the connection source interface:

```
switch(config-msdp-peer) # connect-source 1/1/1
```

Configuring the connection source as ROP:

```
switch(config) # router msdp  
switch(config-msdp) # ip msdp peer 10.1.1.1  
switch(config-msdp-peer) # connect-source 1/1/1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

clear ip msdp peer statistics

```
clear ip msdp peer [all-vrfs | vrf <VRF-NAME> | <PEER-IP>]
```

Description

Clears MSDP SA counters of peer information for the given VRF. If VRF is not specified, it clears SA counters of peers in the default VRF. It also clears MSDP SA counters for a specified peer address.

Parameter	Description
all-vrfs	Clears MSDP peer information for all VRFs. Optional.
vrf <VRF-NAME>	Clears MSDP peer information for a particular VRF. If the <VRF-NAME> is not specified, it clears information for the default VRF. Optional
<PEER-IP>	Clears MSDP peer information for the specified Peer IP. Format: A.B.C.D. Optional.

Examples

Showing MSDP peer information for VRFs:

```
switch# clear ip msdp peer statistics all-vrfs
switch# clear ip msdp peer statistics 2.2.2.2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

description

```
description <TEXT>
no description
```

Description

Configures a description for a specified MSDP peer to make it easier to identify in a configuration or show command output.

The **no** form of this command removes the peer description.

Parameter	Description
<TEXT>	Specifies a description for the MSDP Peer.

Example

Configuring the MSDP peer description:

```
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# description Peer_1
switch(config-msdp-peer)# no description
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables MSDP peer on the L3 interface.

Example

Disabling MSDP peering:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

enable (ip msdp peer)

enable

Description

Enables MSDP peer on the L3 interface.



Only one MSDP peering session per VRF should be configured between two routers to avoid loops.

Example

Enabling MSDP peering:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

ip msdp peer

```
ip msdp peer <IP-ADDR>
no ip msdp peer
```

Description

Changes the current context to the MSDP peer context.

The **no** form of this command removes the MSDP peer configuration from the specified context.

Parameter	Description
<IP-ADDR>	Specifies the IPv4 address of the MSDP peer. Format: A.B.C.D

Examples

Enabling the MSDP peer context:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp	Administrators or local user group members with execution rights for this command.

keepalive

```
keepalive <KEEPALIVE-INTERVAL> <HOLD-TIME>
no keepalive
```

Description

Configures the interval at which a MSDP peer will send keepalive messages, and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.

The **no** form of this command removes the currently configured value and sets it to the default value.

Parameter	Description
<KEEPALIVE-INTERVAL>	Specifies the value for the keepalive interval.
<HOLD-TIME>	Specifies the value for the hold time.

Example

Configuring the keepalive interval and the hold time for MSDP peer:

```
switch(config-msdp-peer) # keepalive 30 45  
switch(config-msdp-peer) # no keepalive
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

mesh-group

```
mesh-group <MESH-NAME>  
no mesh-group <MESH-NAME>
```

Description

Associates the given mesh group with the MSDP peer. This feature is used to reduce the amount of SA traffic in an intra-domain setting.

The **no** form of this command removes the peer from the currently configured mesh.

Parameter	Description
<MESH-NAME>	Specifies the MSDP mesh group name.

Usage

All MSDP peers on the router that participate in the mesh group must be fully meshed with all other peers in the mesh group. When MSDP mesh groups are used, SA messages are not flooded to other mesh group peers. It also eliminates RPF checks on arriving SA messages. With MSDP mesh group configured, SA messages are always accepted from mesh group peers.

Example

Associating a mesh group with an MSDP peer:

```
switch(config-msdp-peer) # mesh-group test-mesh-group
```

Removing the MSDP peer from the configured mesh:

```
switch(config-msdp-peer) # no mesh-group test-mesh-group
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

password (router msdp)

```
password {ciphertext | plaintext} <password>  
no password
```

Description

Enables MD5 password encryption for a TCP connection between two MSDP peers.

The **no** form of this command removes MD5 password encryption.

Parameter	Description
{ciphertext plaintext}	Selects the password type.
<password>	Specifies the password.



When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Configuring MD5 password encryption with a provided plaintext password:

```
switch(config)# router msdp  
switch(config-msdp)#  
switch(config-msdp)# ip msdp peer 10.1.1.1  
switch(config-msdp-peer)#  
switch(config-msdp-peer)# password plaintext F82#4eva
```

Configuring MD5 password encryption with a prompted plaintext password:

```
switch(config)# router msdp  
switch(config-msdp)#
```

```
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# password
Enter the MD5 password: *****
Re-Enter the MD5 password: *****
```

Removing MD5 password encryption:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# no password
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

sa-filter access-list

```
sa-filter {in|out} access-list <ACL-RULE>
no sa-filter {in|out} access-list <ACL-RULE>
```

Description

Associates the given ACL to filter MSDP SA messages on the peer.

The **no** form of this command removes the currently configured ACL entry.

Parameter	Description
{in out}	Enables the filter for incoming or outgoing SA messages.
<ACL-RULE>	Specifies the ACL rule name.

Usage

By default, the MSDP enabled router forwards all the SA messages, and the peer router processes all the received messages. This command allows the user to configure an ACL on the MSDP peer to filter SA messages. User can prevent the incoming/outgoing SA messages on MSDP router by creating incoming/outgoing filter lists using an ACL.

Example

Filtering incoming SA messages on the MSDP peer for the specified ACL:

```
switch(config-msdp-peer) # sa-filter in access-list msdp_sa_filter1
```

Filtering outgoing SA messages on the MSDP peer for the specified ACL:

```
switch(config-msdp-peer) # sa-filter out access-list msdp_sa_filter2
```

Removing filter on the MSDP peer for the specified ACL:

```
switch(config-msdp-peer) # no sa-filter in access-list msdp_sa_filter2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-msdp-peer	Administrators or local user group members with execution rights for this command.

show ip msdp count

show ip msdp count [all-vrfs | vrf <VRF-NAME>]

Description

Shows MSDP Peer (S,G) learnt count for a given VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows MSDP (S,G) entries count for all VRFs. Optional.
vrf <VRF-NAME>	Shows MSDP (S,G) entries count for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF. Optional.

Examples

Showing the MSDP learnt count:

```
switch# show ip msdp count

VRF: default
SA state per Peer counters
<Peer>:<#SA learned>
10.1.1.1: 30
20.1.1.1: 100
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip msdp peer

show ip msdp peer [all-vrfs | vrf <VRF-NAME> | <PEER-IP>]

Description

Shows MSDP Peer information for the given VRF. Optionally, you can show specific information by VRF.

Parameter	Description
all-vrfs	Shows MSDP peer information for all VRFs. Optional.
vrf <VRF-NAME>	Shows MSDP peer information for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF. Optional.
<PEER-IP>	Shows MSDP Peer information for specified Peer IP. Format: A.B.C.D. Optional.

Examples

Showing MSDP peer information for VRFs:

```
switch# show ip msdp peer

VRF: default

MSDP Peer: 10.1.1.1
Connection status
State: up Resets: 0 Connection Source: 1/1/1
Uptime(Downtime): 0m 25s SA Messages sent: 0
SA's learned from this peer: 0
SA Filtering
Input (S,G) filter: msdp_sa_filter1 (S,G) entries dropped: 0
Output (S,G) filter: msdp_sa_filter2 (S,G) entries dropped: 30
Mesh group: test-mesh-group


switch# show ip msdp peer 20.1.1.1

VRF: default

MSDP Peer: 20.1.1.1
Connection status
State: down Resets: 0 Connection Source: 1/1/2
Uptime(Downtime): 1m 25s SA Messages sent: 0
SA's learned from this peer: 0
SA Filtering
Input (S,G) filter: msdp_sa_filter1 (S,G) entries dropped: 0
Output (S,G) filter: msdp_sa_filter2 (S,G) entries dropped: 20
Mesh group: test-mesh-group
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip msdp sa-cache

```
show ip msdp sa-cache [all-vrfs | vrf <VRF-NAME> | <SRC-OR-GRP-IP>]
```

Description

Shows MSDP Peer SA-Cache information for the given VRF. Optionally, you can show specific information by VRF. The SA-Cache output can be filtered based on the source or group IPv4 address.

Parameter	Description
all-vrfs	Shows MSDP SA-Cache information for all VRFs. Optional.
vrf <VRF-NAME>	Shows MSDP SA-Cache information for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF. Optional.
<SRC-OR-GRP-IP>	Shows the filtered SA-cache output for the specified source or group IPv4 address. Format: A.B.C.D. Optional.

Examples

Showing MSDP SA-Cache information for VRFs:

```
switch# show ip msdp sa-cache

VRF: default
(30.0.0.1, 230.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2
(20.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2
(10.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2

Total entries: 3

switch# show ip msdp sa-cache 229.1.1.1
(20.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2
(10.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2

Total entries: 2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip msdp summary

`show ip msdp summary [all-vrfs | vrf <VRF-NAME>]`

Description

Shows MSDP peer summary for a given VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>all-vrfs</code>	Shows the MSDP peer summary for all VRFs. Optional.
<code>vrf <VRF-NAME></code>	Shows the MSDP peer summary for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF. Optional.

Examples

Showing the MSDP peer summary:

```
switch# show ip msdp summary

VRF: default

MSDP Peer Status Summary
Peer address    State    Uptime(Downtime)    Reset Count    SA Count
10.1.1.1        down    34m 34s              0              0
20.1.1.1        up      50m 24s              0              50
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

clear spanning-tree statistics

```
clear spanning-tree statistics
```

Description

Clears the spanning tree BPDU statistics.

Example

Clearing the spanning tree BPDU statistics:

```
switch(config)# clear spanning-tree statistics
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show spanning-tree

```
show spanning-tree [vsx-peer]
```

Description

Shows priority, address, Hello-time, Max-age, and Forward-delay for bridge and root node.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing spanning tree standard information:

```
switch# show spanning-tree
Spanning tree status      : Enabled Protocol: MSTP

MST0
  Root ID
    Priority      : 0
    MAC-Address: 02:12:12:00:01:00
    This bridge is the root
    Hello time(in seconds):2  Max Age(in seconds):20
    Forward Delay(in seconds):15

  Bridge ID
    Priority      : 0
    MAC-Address: 02:12:12:00:01:00
    Hello time(in seconds):2  Max Age(in seconds):20
    Forward Delay(in seconds):15

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx
TCN-Tx    TCN-Rx
-----
1/1/1     Designated Forwarding 20000     128       P2P Edge  100       60
20        10
1/1/2     Designated Forwarding 20000     128       P2P      100       60
20        10
1/1/3     Designated Forwarding 20000     128       Shr      100       60
20        10
1/1/4     Designated Forwarding 20000     128       Shr Edge  100       60
20        10
1/1/5     Alternate Loop-Inc  20000     128       Shr Edge  100       60
20        10
1/1/6     Alternate Root-Inc  20000     128       Shr Edge  100       60
20        10
1/1/7     Root          Forwarding 2000      128       P2P      100       60
20        10
1/1/8     Alternate Blocking  20000     128       P2P      100       60
20        10
1/1/9     Disabled      Down       20000     128       P2P      100       60
20        10

Number of topology changes      : 4
Last topology change occurred   : 516 seconds ago
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state <code>Down</code> is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree detail

show spanning-tree detail [vsx-peer]

Description

Shows spanning tree detail including CIST and corresponding port information.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing spanning tree detailed information:

```
switch# show spanning-tree detail
Spanning tree status      : Enabled Protocol: MSTP

MST0
  Root ID
    Priority      : 32768, Root
    MAC-Address   : 48:0F:CF:AF:04:76
    Hello time(in seconds):2   Max Age(in seconds):20
    Forward Delay(in seconds):15

  Bridge ID
    Priority      : 32768
    MAC-Address   : 48:0F:CF:AF:04:76
    Hello time(in seconds):2   Max Age(in seconds):20
    Forward Delay(in seconds):15

  PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx
  TCN-Tx    TCN-Rx
  -----
  1/1/1     Designated Forwarding 20000     128       P2P Edge  100       60
  20        10
  1/1/2     Designated Forwarding 20000     128       P2P      100       60
  20        10
  1/1/3     Designated Forwarding 20000     128       Shr      100       60
  20        10
  1/1/4     Designated Forwarding 20000     128       Shr Edge  100       60
  20        10
  1/1/5     Alternate  Loop-Inc  20000     128       Shr Edge  100       60
  20        10
  1/1/6     Alternate  Root-Inc  20000     128       Shr Edge  100       60
  20        10
  1/1/7     Disabled   Down      20000     128       P2P      100       60
  20        10
```

```

Topology change flag      : True
Number of topology changes : 4
Last topology change occurred : 516 seconds ago
Hello expiry             : 1 second
Forward delay expiry      : 18 seconds

Port 1/1/1
Designated root has priority      : 32768      Address:
48:0F:CF:AF:04:76
Designated bridge has priority    : 32768      Address:
48:0F:CF:AF:04:76
Designated port                  : 1/1/1
Number of transitions to forwarding state : 3
BPDUs sent                      : 347
BPDUs received                  : 9
TCN_Tx: 20, TCN_Rx: 10

Port 1/1/2
Designated root has priority      : 32768      Address:
48:0F:CF:AF:04:76
Designated bridge has priority    : 32768      Address:
48:0F:CF:AF:04:76
Designated port                  : 1/1/2
Number of transitions to forwarding state : 3
BPDUs sent                      : 350
BPDUs received                  : 11
TCN_Tx: 20, TCN_Rx: 10

Port lag1 ID 321
Designated root has priority      : 32768      Address:
48:0F:CF:AF:04:76
Designated bridge has priority    : 32768      Address:
48:0F:CF:AF:04:76
Designated port id               : 321
Multi-Chassis role               : active
Number of transitions to forwarding state : 3
BPDUs sent                      : 340
BPDUs received                  : 5
TCN_Tx: 20, TCN_Rx: 10

```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state <code>Down</code> is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree inconsistent-ports

`show spanning-tree inconsistent-ports [instance <INSTANCE-ID>]`

Description

Shows ports blocked by STP protection functions such as Root guard, Loop guard, BPDU guard, and RPVST guard in addition to MSTI information.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance ID. Range: 1 to 4094.

Example

Showing spanning tree inconsistent ports:

```
switch# show spanning-tree inconsistent-ports
Instance ID  Blocked Port  Reason
-----
0            1/1/13         BPDU Guard
```

Showing inconsistent port information for instances 1-4:

```
switch# show spanning-tree inconsistent-ports instance 1-4
Instance ID  Blocked Port  Reason
-----
1            1/1/3         Root Guard
2            1/1/7         BPDU Guard
3            1/1/9         Loop Guard
4            1/1/37        RPVST Guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree mst

show spanning-tree mst [vsx-peer]

Description

Shows MSTP configuration and status information for each instance.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing MSTP configuration and status information:

```
switch# show spanning-tree mst
#### MST0
Vlans mapped      : 2,4-4094
Bridge Address    : 48:0F:CF:AF:04:76
Priority          : 32768
Root
Regional Root
Operational      Hello time      : 2 seconds          Forward delay: 15 seconds
                  Max-age        : 20 seconds          TxHoldCount  : 6 pps
Configured       Hello time      : 2 seconds          Forward delay: 15 seconds
                  Max-age        : 20 seconds          Max-Hops     : 20
Root             Address         : 48:0F:CF:AF:04:76      Priority      : 32768
                  Port           : 0                    Path cost    : 0
Regional Root    Address         : 48:0F:CF:AF:04:76      Priority      : 32768
                  Internal cost: 0                      Rem Hops     : 20

PORT    ROLE    STATE    COST    PRIORITY  TYPE    BPDU-Tx  BPDU-Rx
TCN-Tx  TCN-Rx
-----
1/1/1   Designated Forwarding 20000    128      P2P Edge 100      60
20      10
1/1/2   Designated Forwarding 20000    128      P2P      100      60
20      10
1/1/3   Designated Forwarding 20000    128      Shr      100      60
20      10
1/1/4   Designated Forwarding 20000    128      Shr Edge 100      60
20      10
1/1/5   Alternate Loop-Inc  20000    128      Shr Edge 100      60
20      10
1/1/6   Alternate Root-Inc 20000    128      Shr Edge 100      60
20      10
1/1/7   Disabled  Down     20000    128      P2P      100      60
20      10
```


Topology change flag : True
 Number of topology changes : 4
 Last topology change occurred : 516 seconds ago

MST1

Vlans mapped: 1
 Bridge Address : 48:0F:CF:AF:04:76 Priority: 32768
 Root Address : 48:0F:CF:AF:04:76 Priority: 32768
 Port : 0 Cost : 0
 Rem Hops: 20

PORT TCN-Tx	ROLE TCN-Rx	STATE	COST	PRIORITY	TYPE	BPDU-Tx	BPDU-Rx
1/1/1 20	Designated 10	Forwarding	20000	128	P2P Edge	100	60
1/1/2 20	Designated 10	Forwarding	20000	128	P2P	100	60
1/1/3 20	Designated 10	Forwarding	20000	128	Shr	100	60
1/1/4 20	Designated 10	Forwarding	20000	128	Shr Edge	100	60
1/1/5 20	Alternate 10	Loop-Inc	20000	128	Shr Edge	100	60
1/1/6 20	Alternate 10	Root-Inc	20000	128	Shr Edge	100	60
1/1/7 20	Disabled 10	Down	20000	128	P2P	100	60

Topology change flag : True
 Number of topology changes : 4
 Last topology change occurred : 516 seconds ago

MST2

Vlans mapped: 3
 Bridge Address : 48:0F:CF:AF:04:76 Priority: 32768
 Root Address : 48:0F:CF:AF:04:76 Priority: 32768
 Port : 0 Cost : 0
 Rem Hops: 20

PORT TCN-Tx	ROLE TCN-Rx	STATE	COST	PRIORITY	TYPE	BPDU-Tx	BPDU-Rx
1/1/1 20	Designated 10	Forwarding	20000	128	P2P Edge	100	60
1/1/2 20	Designated 10	Forwarding	20000	128	P2P	100	60
1/1/3 20	Designated 10	Forwarding	20000	128	Shr	100	60
1/1/4 20	Designated 10	Forwarding	20000	128	Shr Edge	100	60
1/1/5 20	Alternate 10	Loop-Inc	20000	128	Shr Edge	100	60
1/1/6 20	Alternate 10	Root-Inc	20000	128	Shr Edge	100	60

Topology change flag : True
 Number of topology changes : 4

Last topology change occurred : 516 seconds ago



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state <code>Down</code> is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree mst-config

`show spanning-tree mst-config [vsx-peer]`

Description

Shows MSTP instance and corresponding VLAN information.

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing configuration information for MST instances and corresponding VLANs:

```
switch# show spanning-tree mst-config
MST configuration information
  MST config ID       : reg
  MST config revision  : 1
  MST config digest    : 2D2BC9A32097B463C48EE1817673FA2D
  Number of instances  : 2

Instance ID    Member VLANs
-----
0              2,4-4094
1              1
2              3
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree mst detail

show spanning-tree mst detail [vsx-peer]

Description

Shows detailed information for all MST instances.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing detailed information for all MST instances:

```
switch# show spanning-tree mst detail
#### MST0
Vlans mapped: 2,4-4094
Bridge      Address: 48:0F:CF:AF:04:76      Priority: 32768
Root
Regional Root
Operational  Hello time    : 2 seconds          Forward delay: 15 seconds
              Max-age      : 20 seconds          TxHoldCount  : 6 pps
Configured   Hello time    : 2 seconds          Forward delay: 15 seconds
              Max-age      : 20 seconds          Max-Hops     : 20
Root         Address     : 48:0F:CF:AF:04:76      Priority      : 32768
              Port        : 0                  Path cost    : 0
Regional Root Address     : 48:0F:CF:AF:04:76      Priority      : 32768
              Internal cost: 0                  Rem Hops     : 20

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx      BPDU-Rx
TCN-Tx    TCN-Rx
-----
```

```

-- -----
1/1/1    Designated Forwarding 20000    128      P2P Edge  100      60
  20      10
1/1/2    Designated Forwarding 20000    128      P2P      100      60
  20      10
1/1/3    Designated Forwarding 20000    128      Shr      100      60
  20      10
1/1/4    Designated Forwarding 20000    128      Shr Edge  100      60
  20      10
1/1/5    Alternate Loop-Inc   20000    128      Shr Edge  100      60
  20      10
1/1/6    Alternate Root-Inc   20000    128      Shr Edge  100      60
  20      10
1/1/7    Disabled   Down      20000    128      P2P      100      60
  20      10

```

```

Topology change flag      : True
Number of topology changes : 4
Last topology change occurred : 516 seconds ago

```

```

Port 1/1/1
Designated root address      : 48:0F:CF:AF:04:76
Designated regional root address : 48:0F:CF:AF:04:76
Designated bridge address    : 48:0F:CF:AF:04:76
Priority                      : 32768
BPDUs sent                   : 638
BPDUs received               : 9
Message expiry                : 1 second
Forward delay expiry         : 18 seconds
Forward transitions           : 3
TCN_Tx: 10, TCN_Rx: 10

```

```

Port 1/1/2
Designated root address      : 48:0F:CF:AF:04:76
Designated regional root address : 48:0F:CF:AF:04:76
Designated bridge address    : 48:0F:CF:AF:04:76
Priority                      : 32768
BPDUs sent                   : 641
BPDUs received               : 11
Message expiry                : 1 second
Forward delay expiry         : 18 seconds
Forward transitions           : 3
TCN_Tx: 10, TCN_Rx: 10

```

```

#### MST1
Vlans mapped: 1
Bridge      Address : 48:0F:CF:AF:04:76      Priority: 32768
Root        Address : 48:0F:CF:AF:04:76      Priority: 32768
            Port    : 0                      Cost    : 0
            Rem Hops: 20

```

PORT	ROLE	STATE	COST	PRIORITY	TYPE	BPDU-Tx	BPDU-Rx
TCN-Tx	TCN-Rx						
1/1/1	Designated	Forwarding	20000	128	P2P Edge	100	60
20	10						
1/1/2	Designated	Forwarding	20000	128	P2P	100	60
20	10						
1/1/3	Designated	Forwarding	20000	128	Shr	100	60
20	10						
1/1/4	Designated	Forwarding	20000	128	Shr Edge	100	60

```

    20          10
1/1/5  Alternate Loop-Inc  20000    128      Shr Edge  100      60
    20          10
1/1/6  Alternate Root-Inc  20000    128      Shr Edge  100      60
    20          10
1/1/7  Disabled  Down      20000    128      P2P      100      60
    20          10

```

```

Topology change flag      : True
Number of topology changes : 4
Last topology change occurred : 516 seconds ago

```

```

Port 1/1/1
Designated root address      : 48:0F:CF:AF:04:76
Designated bridge address    : 48:0F:CF:AF:04:76
Priority                      : 32768
BPDUs sent                   : 638
BPDUs received               : 9
Message expiry               : 1 second
Forward delay expiry         : 18 seconds
Forward transitions          : 4
TCN_Tx: 10, TCN_Rx: 10

```

```

Port 1/1/2
Designated root address      : 48:0F:CF:AF:04:76
Designated bridge address    : 48:0F:CF:AF:04:76
Priority                      : 32768
BPDUs sent                   : 641
BPDUs received               : 11
Message expiry               : 1 second
Forward delay expiry         : 18 seconds
Forward transitions          : 4
TCN_Tx: 10, TCN_Rx: 10

```

MST2

```

Vlans mapped: 3
Bridge      Address : 48:0F:CF:AF:04:76      Priority: 32768
Root       Address : 48:0F:CF:AF:04:76      Priority: 32768
          Port      : 0                      Cost      : 0
          Rem Hops: 20

```

PORT	ROLE	STATE	COST	PRIORITY	TYPE	BPDU-Tx	BPDU-Rx
TCN-Tx	TCN-Rx						
1/1/1	Designated	Forwarding	20000	128	P2P Edge	100	60
20	10						
1/1/2	Designated	Forwarding	20000	128	P2P	100	60
20	10						
1/1/3	Designated	Forwarding	20000	128	Shr	100	60
20	10						
1/1/4	Designated	Forwarding	20000	128	Shr Edge	100	60
20	10						
1/1/5	Alternate	Loop-Inc	20000	128	Shr Edge	100	60
20	10						
1/1/6	Alternate	Root-Inc	20000	128	Shr Edge	100	60
20	10						
1/1/7	Disabled	Down	20000	128	P2P	100	60
20	10						

```

Topology change flag      : True

```

```

Number of topology changes      : 4
Last topology change occurred  : 516 seconds ago

Port 1/1/1
Designated root address         : 48:0F:CF:AF:04:76
Designated bridge address       : 48:0F:CF:AF:04:76
Priority                         : 32768
BPDUs sent                      : 638
BPDUs received                  : 9
Message expiry                  : 1 second
Forward delay expiry            : 18 seconds
Forward transitions              : 3
TCN_Tx: 10, TCN_Rx: 10

Port 1/1/2
Designated root address         : 48:0F:CF:AF:04:76
Designated bridge address       : 48:0F:CF:AF:04:76
Priority                         : 32768
BPDUs sent                      : 641
BPDUs received                  : 11
Message expiry                  : 1 second
Forward delay expiry            : 18 seconds
Forward transitions              : 3
TCN_Tx: 10, TCN_Rx: 10

```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree mst <INSTANCE-ID>

show spanning-tree mst <INSTANCE-ID> [vsx-peer]

Description

Displays MSTP configurations for the given instance ID.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 0 to 4094.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show spanning-tree mst 1

#### MST1
Vlans mapped: 1
Bridge      Address : 48:0F:CF:AF:04:76      Priority: 32768
Root        Address : 48:0F:CF:AF:04:76      Priority: 32768
            Port      : 0              Cost      : 0
            Rem Hops: 20

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx
TCN-Tx    TCN-Rx
-----
1/1/1     Designated Forwarding 20000     128       P2P Edge 100       60
20        10
1/1/2     Designated Forwarding 20000     128       P2P      100       60
20        10
1/1/3     Designated Forwarding 20000     128       Shr      100       60
20        10
1/1/4     Designated Forwarding 20000     128       Shr Edge 100       60
20        10
1/1/5     Alternate  Loop-Inc  20000     128       Shr Edge 100       60
20        10
1/1/6     Alternate  Root-Inc  20000     128       Shr Edge 100       60
20        10
1/1/7     Disabled   Down      20000     128       P2P Bound 100       60
20        10

Topology change flag      : True
Number of topology changes : 4
Last topology change occurred : 516 seconds ago
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree mst <INSTANCE-ID> detail

show spanning-tree mst <INSTANCE-ID> detail [vsx-peer]

Description

Displays MSTP configurations for the given instance ID with corresponding port details.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 0 to 4094.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show spanning-tree mst 1 detail

#### MST1
Vlans mapped: 1
Bridge      Address : 48:0F:CF:AF:04:76      Priority: 32768
Root        Address : 48:0F:CF:AF:04:76      Priority: 32768
            Port      : 0              Cost      : 0
            Rem Hops: 20

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx
TCN-Tx    TCN-Rx
-----
--
1/1/1     Designated Forwarding 20000     128       P2P Edge  100       60
20        10
1/1/2     Designated Forwarding 20000     128       P2P      100       60
20        10
1/1/3     Designated Forwarding 20000     128       Shr      100       60
20        10
1/1/4     Designated Forwarding 20000     128       Shr Edge  100       60
20        10
1/1/5     Alternate  Loop-Inc  20000     128       Shr Edge  100       60
20        10
1/1/6     Alternate  Root-Inc  20000     128       Shr Edge  100       60
20        10
1/1/7     Disabled   Down      20000     128       P2P Bound 100       60
20        10

Topology change flag      : True
Number of topology changes : 4
Last topology change occurred : 516 seconds ago
```



```

Port 1/1/1
Designated root address      : 48:0F:CF:AF:04:76
Designated bridge address    : 48:0F:CF:AF:04:76
Priority                      : 32768
BPDUs sent                   : 667
BPDUs received               : 9
Message expiry               : 0 second
Forward delay expiry         : 18 seconds
Forward transitions          : 4
TCN_Tx: 10, TCN_Rx: 10

Port 1/1/2
Designated root address      : 48:0F:CF:AF:04:76
Designated bridge address    : 48:0F:CF:AF:04:76
Priority                      : 32768
BPDUs sent                   : 670
BPDUs received               : 11
Message expiry               : 0 second
Forward delay expiry         : 18 seconds
Forward transitions          : 4
TCN_Tx: 10, TCN_Rx: 10

```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree mst interface

show spanning-tree mst <INSTANCE-ID> interface <IFNAME> [vsx-peer]

Description

Shows MSTP configurations for the given instance ID with corresponding port details.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 0 to 4094.
<IFNAME>	Specifies an interface.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing MST configuration and port details:

```
switch# show spanning-tree mst 1 interface 1/1/1
Port 1/1/1
```

Instance	Role	State	Cost	Priority	Vlans mapped
1	Designated	Forwarding	20000	128	1



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree summary port

show spanning-tree summary port

Description

Shows spanning tree port summary information.

Example

Showing summary of spanning tree ports:

```
switch# show spanning-tree summary port
```

STP status	: Enabled
Protocol	: MSTP
BPDU guard timeout value	: None

```

BPDU guard enabled interfaces : 1/1/1-1/1/9,1/1/11,1/1/13,1/1/15,1/1/17,1/1/19,
                               1/1/21,lag1,lag2
BPDU filter enabled interfaces : None
Root guard enabled interfaces : 1/1/3
Loop guard enabled interfaces : 1/1/2
TCN guard enabled interfaces  : 1/1/1-1/1/3
RPVST filter enabled interfaces : 1/1/37
RPVST guard enabled interfaces : None

```

Interface count by state

Instance ID	Blocking	Listening	Learning	Forwarding	Down
0	2	0	0	15	0
1	2	0	0	15	0
2	2	0	0	15	0
Total = 3	6	0	0	45	0



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state <code>Down</code> is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree summary root

```
show spanning-tree summary root
```

Description

Shows spanning tree root summary information.

Example

Showing spanning tree root summary:

```

switch# show spanning-tree summary root

STP status          : Enabled
Protocol            : MSTP

```

System ID : 70:72:cf:32:50:f5

Root bridge for STP Instance : 0,1,2

Instance ID	Priority	Root ID	Root cost	Hello Time	Max Age	Fwd Dly	Root Port
0	32768	70:72:cf:32:50:f5	0	2	20	15	n/a
1	32768	70:72:cf:32:50:f5	0	2	20	15	n/a
2	32768	70:72:cf:32:50:f5	200	2	20	15	1/1/1



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

spanning-tree

spanning-tree
no spanning-tree

Description

Enables the spanning tree protocol on the switch.

The **no** form of this command disables the spanning tree protocol on the switch.

Examples

Enabling spanning tree:

```
switch(config)# spanning-tree
```

Disabling spanning tree:

```
switch(config)# no spanning-tree
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree bpd-filter

spanning-tree bpd-filter
no spanning-tree bpd-filter

Description

Enables the bpd filter for the interface.

The BPDU filter feature allows control of spanning tree participation on a per-port basis. It can be used to exclude specific ports from becoming part of spanning tree operations. A port with the BPDU filter enabled will ignore incoming BPDU packets, does not transmit BPDU, and stays locked in the spanning tree forwarding state. All other ports maintain their role. Typical uses for this parameter include:

- To have MSTP operations running on selected ports of the switch rather than every port of the switch at a time.
- To prevent the spread of errant BPDU frames.
- To eliminate the need for a topology change when a port's link status changes. For example, ports that connect to servers and workstations can be configured to remain outside of spanning tree operations.
- To protect the network from denial of service attacks that use spoofing BPDUs by dropping incoming BPDU frames. For this scenario, BPDU protection offers a more secure alternative, implementing port shut down and a detection alert when errant BPDU frames are received.



Ports configured with the BPDU filter mode remain active (learning and forward frames). However, spanning tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, redundant links) using these ports. If you suddenly have a high load, disconnect the link and disable the BPDU filter (using the no command.)

The **no** form of the command sets the bpd filter status to the default of disabled on the interface.

Examples

Enabling the bpd filter on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree bpd-filter
```

Disabling bpd filter on interface 1/1/1:

```
switch(config)# interface 1/1/1  
switch(config-if)# no spanning-tree bpdu-filter
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree bpdu-guard

```
spanning-tree bpdu-guard  
no spanning-tree bpdu-guard
```

Description

Enables the BPDU guard on the selected switch interface. When BPDU guard is enabled, interfaces receiving MSTP BPDUs become disabled.

BPDU protection is a security feature designed to protect the active MSTP topology by preventing spoofed BPDU packets from entering the MSTP domain. In a typical implementation, BPDU protection would be applied to edge ports connected to end user devices that do not run MSTP. If MSTP BPDU packets are received on a protected port, this feature disables that port and alerts the network manager using an SNMP trap.

Occasionally a hardware or software failure can cause MSTP to fail, creating forwarding loops that can cause network failures where unidirectional links are used. The non-designated port transitions in a faulty manner because the port is no longer receiving MSTP BPDUs.

The **no** form of the command disables BPDU guard on the selected interface.

Examples

Enabling the BPDU guard on interface 1/1/1:

```
switch(config)# interface 1/1/1  
switch(config-if)# spanning-tree bpdu-guard
```

Disabling BPDU guard on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree bpdu-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree bpdu-guard timeout

```
spanning-tree bpdu-guard timeout <INTERVAL>
no spanning-tree bpdu-guard timeout [<INTERVAL>]
```

Description

Enables and configures the auto re-enable timeout in seconds for all interfaces with BPDU guard enabled. When an interface is disabled after receiving an unauthorized BPDU it will automatically be re-enabled after the timeout expires. The default is for the interface to stay disabled until manually re-enabled.

The **no** form of the command disables BPDU guard timeout. This is the default.

Parameter	Description
<INTERVAL>	Specifies the re-enable timeout in seconds. Range: 1 to 65535.

Example

Enabling the BPDU guard timeout:

```
switch(config)# spanning-tree bpdu-guard timeout 10
```

Disabling BPDU guard timeout:

```
switch(config)# no spanning-tree bpdu-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree config-name

spanning-tree config-name <CONFIG-NAME>
no spanning-tree config-name [<CONFIG-NAME>]

Description

Sets the configuration name for the MST region in which the switch resides.

All switches within an MST region must have identical configuration names. For more than one MSTP switch in the same MST region, the identical region name must be configured on all such switches. If the default configuration name is retained on a switch, it cannot exist in the same MST region with another switch.

The **no** form of this command overwrites the currently configured name with the default name. The default name is a text string using the hexadecimal representation of the system MAC address.

Parameter	Description
<CONFIG-NAME>	Specifies the configuration name for the MST region in which the switch resides. Default: text string using the hexadecimal representation of the MAC address of the switch. Range: 1 - 32 nonblank characters (case-sensitive).

Examples

Setting the configuration name to MST0:

```
switch(config)# spanning-tree config-name MST0
```

Setting the configuration name to the default value:

```
switch(config)# no spanning-tree config-name
```




For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree config-revision

```
spanning-tree config-revision <REVISION-NUMBER>
no spanning-tree config-revision [<REVISION-NUMBER>]
```

Description

Configures the revision number for the MST region in which the switch resides. All switches within an MST region must have identical revision numbers. Use this setting to differentiate between region configurations. For example, when changing configuration settings within a region where you want to track the configuration versions you use, or when creating a new region from a subset of switches in a current region and you want to maintain the same region name.

The **no** form of this command overwrites the currently configured revision number of the MST region and sets it to the default value of 0.

Parameter	Description
<REVISION-NUMBER>	Specifies the revision number for the MST region in which the switch resides. Range: 0 - 65535. Default: 0.

Examples

Setting the revision to 40:

```
switch(config)# spanning-tree config-revision 40
```

Setting the revision to the default value:

```
switch(config)# no spanning-tree config-revision
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree cost

```
spanning-tree cost <PORT-COST>
no spanning-tree cost [<PORT-COST>]
```

Description

Sets individual port cost for MSTI 0.

For a given port, the path cost setting can be different for different MSTIs to which the port may belong. The switch uses the path cost to determine which ports are the forwarding ports in the MSTI; that is, which links to use for the active topology of the MSTI and which ports to block.

Cost gets calculated based on physical interface link speed. It is not based on cumulative speed of all physical links under a lag. Therefore, the cost will be same for a 1G interface and 2x1G lag interfaces.

The **no** form of the command sets the port cost for MSTI 0 instance to the default value.

Parameter	Description
<PORT-COST>	Specifies the cost of the port for MSTI 0. Range: 1-200,000,000. Default is calculated from the port link speed: 10 Mbps link speed equals a path cost of 2,000,000. 100 Mbps link speed equals a path cost of 200,000. 1 Gbps link speed equals a path cost of 20,000. 10 Gbps link speed equals a path cost of 2,000. 100 Gbps link speed equals a path cost of 200. 1 Tbps link speed equals a path cost of 20.

Examples

Setting the cost to **2000** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree cost 2000
```

Setting the cost to the default on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree cost
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree forward-delay

```
spanning-tree forward-delay <DELAY-IN-SECS>
no spanning-tree forward-delay [<DELAY-IN-SECS>]
```

Description

Configures the time the switch waits between transitions from listening to learning and from learning to forwarding states.

The **no** form of this command sets forward delay time for the bridge to the default of 15 seconds.

Parameter	Description
<DELAY-IN-SECS>	Specifies the forward delay time in seconds. Default: 15 seconds. Range: 4-30.

Examples

Setting forward delay to 6 seconds:

```
switch(config)# spanning-tree forward-delay 6
```

Setting forward delay to the default of 15 seconds:

```
switch(config)# no spanning-tree forward-delay
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree hello-time

```
spanning-tree hello-time <HELLO-IN-SECS>
no spanning-tree hello-time [<HELLO-IN-SECS>]
```

Description

Configures the transmission interval between consecutive Bridge Protocol Data Units (BPDU) that the switch sends as a root bridge. The hello time interval is inserted in outbound BPDUs.

The **no** form of this command sets hello time to the default of 2 seconds.

Parameter	Description
<HELLO-IN-SECS>	Specifies the hello time interval in seconds. Default: 2 seconds. Range: 2-10.

Examples

Setting the hello time interval to 6 seconds:

```
switch(config)# spanning-tree hello-time 6
```

Setting the hello time interval to the default of 2 seconds:

```
switch(config)# no spanning-tree hello-time
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree instance cost

```
spanning-tree instance <INSTANCE-ID> cost <PORT-COST>
no spanning-tree instance <INSTANCE-ID> cost [<PORT-COST>]
```

Description

Sets the individual port cost for an MSTI. The switch uses the path cost to determine which links to use for the active topology of the MSTI (forwarding ports) and which ports to block. The path cost setting for a port can be different on each MSTI to which the port belongs.

The **no** form of this command sets the port cost for an MSTI to the default value.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTI number. Range: 1- 4094.
<PORT-COST>	Specifies the cost of the port for the MSTI. Range: 1-200000000. Default value is calculated from the port link speed: 10 Mbps link speed equals a path cost of 2000000. 100 Mbps link speed equals a path cost of 200000. 1 Gbps link speed equals a path cost of 20000.

Examples

Setting the port **1/1/1** cost for MSTI **1** to **2000**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree instance 1 cost 2000
```

Setting the port **1/1/1** cost for MSTI **1** to the default:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree instance 1 cost
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree instance port-priority

spanning-tree instance <INSTANCE-ID> port-priority <PRIORITY-MULTIPLIER>
no spanning-tree instance <INSTANCE-ID> port-priority [<PRIORITY-MULTIPLIER>]

Description

Configures the priority as a priority multiplier for the specified ports in the specified MST instance. For a given port, the priority setting can be different for different MST instances to which the port may belong.

The **no** form of this command sets the port priority to the default value of 8 for the MST instance. The default priority value is derived by multiplying 8 by 16.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 1- 4094.
<PRIORITY-MULTIPLIER>	Specifies the priority as a multiplier. Default: 8. Range: 0 to 15. The priority range for a port in a given MST instance is 0 to 255. However, this command specifies the priority as a multiplier (0 to 15) of 16. When you specify a priority multiplier of 0 to 15, the actual priority assigned to the switch is: (priority-multiplier) x 16.

Examples

Setting the port **1/1/1** priority for instance **1** to **8**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree instance 1 port-priority 8
```

Setting the port 1/1/1 priority for instance 1 to the default:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree instance 1 port-priority
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree instance priority

```
spanning-tree instance <INSTANCE-ID> priority <PRIORITY-MULTIPLIER>
no spanning-tree instance <INSTANCE-ID> priority [<PRIORITY-MULTIPLIER>]
```

Description

Sets the switch priority for the specified MST instance.

The **no** form of this command sets the priority for the specified instance to the default of 8.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 1 to 4094.
<PRIORITY-MULTIPLIER>	Specifies the priority as a multiplier. Default: 8. Range: 0 to 15. The priority range for an MSTP switch is 0-61440. However, this command specifies the priority as a multiplier (0 - 15) of 4096. That is, when you specify a priority multiplier value of 0 - 15, the actual priority assigned to the switch is: (priority-multiplier) x 4096. For example, with 2 as the priority-multiplier on a given MSTP switch, the switch priority setting is 8,192.

Examples

Setting the priority multiplier for instance 1 to 5:

```
switch(config)# spanning-tree instance 1 priority 5
```

Setting the priority multiplier for instance 1 to the default of 8:

```
switch(config)# no spanning-tree instance 1 priority
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree instance vlan

```
spanning-tree instance <INSTANCE-ID> vlan <VLAN-ID>
no spanning-tree instance <INSTANCE-ID> vlan <VLAN-ID>
```

Description

Creates a new instance with VLANs mapped or maps VLANs to an existing instance.

Each instance must have at least one VLAN mapped to it. When VLANs are mapped to an instance, they are automatically unmapped from the instance they were mapped to before. Any MSTP instance can have all the VLANs configured on the switch.

The **no** form of this command removes the specified VLAN from the MSTP instance.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 1 to 4094.
<VLAN-ID>	Specifies a VLAN ID number.

Examples

Mapping VLAN 1 to instance 1:

```
switch(config)# spanning-tree instance 1 vlan 1
```

Removing VLAN 1 from instance 1:

```
switch(config)# no spanning-tree instance 1 vlan 1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree link-type

spanning-tree link-type {point-to-point|shared}

Description

Specifies the link type of the interface, which is normally derived from the duplex setting of the port. The default setting depends on the duplex mode of the port: full-duplex ports are point-to-point, half-duplex ports are shared.

Parameter	Description
point-to-point	Specifies the link type as point-to-point.
shared	Specifies the link type as shared.

Examples

Setting the link type to point-to-point on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree link-type point-to-point
```

Setting the link type to shared on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree link-type shared
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree loop-guard

spanning-tree loop-guard
no spanning-tree loop-guard

Description

Enables the loop guard on the interface. STP loop guard is best applied on blocking or forwarding ports.

The **no** form of the command sets the loop guard status to the default of disabled on the interface.

Usage

Occasionally a hardware or software failure can cause MSTP to fail, creating forwarding loops that can cause network failures where unidirectional links are used. The non-designated port transitions in a faulty manner because the port is no longer receiving MSTP BPDUs.

Loop guard causes the non-designated port to go into the MSTP loop inconsistent state instead of the forwarding state. In the loop inconsistent state the port prevents data traffic and BPDU transmission through the link, therefore avoiding the loop creation. When BPDUs again are received on the inconsistent port, it resumes normal MSTP operation automatically.

In this example, the transmission from switch 1 port 10 to switch 2 port 20 is blocked due to a hardware failure. Switch 2 port 2 does not receive BPDUs and goes into a forwarding state, creating a loop.

When loop guard is configured for switch 2 port 20, this port goes from a forwarding state to an inconsistent state, and does not forward the traffic through the link, thus avoiding loop creation.

Examples

Enabling the loop guard on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree loop-guard
```

Disabling loop guard on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree loop-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree max-age

```
spanning-tree max-age <AGE-IN-SECS>
no spanning-tree max-age [<AGE-IN-SECS>]
```

Description

Sets the maximum age timer, which specifies the maximum age value that the switch inserts in outbound BPDU packets it sends as a root bridge. Max-age is the interval, specified in the BPDU, that BPDU data remains valid after its reception.

The bridge recomputes the spanning tree topology if it does not receive a new BPDU before max-age expiry.

The **no** form of this command sets the max-age value to the default of 20 seconds.

Parameter	Description
<code><AGE-IN-SECS></code>	Specifies the max-age in seconds. Range: 6 to 40. Default: 20.

Examples

Setting the max-age to 10 seconds:

```
switch(config)# spanning-tree max-age 10
```

Setting the max-age to the default of 20 seconds:

```
switch(config)# no spanning-tree max-age
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree max-hops

```
spanning-tree max-hops <HOP-COUNT>  
no spanning-tree max-hops [<HOP-COUNT>]
```

Description

Configures the max hop setting that the switch inserts into BPDUs that it sends out as the root bridge. The max hop setting determines the number of bridges in an MST region that a BPDU can traverse before it is discarded.

The **no** form of this command sets the maximum number of hops to the default of 20.

Parameter	Description
<HOP-COUNT>	Specifies the maximum number of hops. Range: 1 to 40. Default: 20.

Examples

Setting the hop count to 10:

```
switch(config)# spanning-tree max-hops 10
```

Setting the max-age to the default of 20:

```
switch(config)# no spanning-tree max-hops
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree mode

```
spanning-tree mode {mstp|rpvst [auto-vlan-enable [priority <NUMBER>]]}
no spanning-tree mode {mstp|rpvst [auto-vlan-enable [priority <NUMBER>]]}
```

Description

Sets the spanning tree protocol (STP) mode to either MSTP mode (Multiple-instance Spanning Tree Protocol) or RPVST mode (Rapid Per VLAN Spanning Tree). Enabling the RPVST Auto VLAN feature will run RPVST on all VLANs currently configured on the switch. Default priority of 8 will be assigned to the VLANs being auto created.

The **no** form of this command sets the spanning tree mode to the default **mstp**.



Enabling auto-VLAN can lead to an undeterministic state if auto scaled beyond the max system limit mentioned in the capacity-status.

Parameter	Description
mstp	Sets the STP mode to MSTP which applies spanning tree separately for each set of VLANs called an MSTI (multiple spanning tree instance).
rpvst	Sets the STP mode to RPVST.
auto-vlan-enable	Selects RPVST auto VLAN mode.
priority <NUMBER>	Specifies the priorities for all auto created RPVST instances. Configured as a multiple of 4096. Default: 8.

Examples

Enabling MSTP mode:

```
switch(config) # spanning-tree mode mstp
```

Disabling MSTP mode:

```
switch(config) # no spanning-tree mode mstp
```

Enabling RPVST mode:

```
switch(config) # spanning-tree mode rpvst
```

Disabling RPVST mode:

```
switch(config) # no spanning-tree mode rpvst
```

Enabling RPVST auto VLAN with a priority of 1:

```
switch(config) # spanning-tree mode rpvst auto-vlan-enable priority 1
```

Disabling RPVST auto VLAN with a priority of 1:

```
switch(config) # no spanning-tree mode rpvst auto-vlan-enable priority 1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.12.1000	Auto VLAN enable added.

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree port-priority

```
spanning-tree port-priority <PRIORITY-MULTIPLIER>
no spanning-tree port-priority [<PRIORITY-MULTIPLIER>]
```

Description

Configures the port priority. The priority of a port can be different for each MST instance to which it belongs.

The **no** form of the command sets the port priority for MST instance 0 to the default of 8. The default priority value is derived by multiplying 8 by 8. For LAG interfaces the default is 4.

Parameter	Description
<PRIORITY-MULTIPLIER>	Specifies the port priority as a multiplier. Default: 8, except for LAG interfaces where the default is 4. Range: 0 to15. The priority range for a port in a given MSTI is 0 to 255. However, this command specifies the priority as a multiplier (0 to 15) of 16. When you specify a priority multiplier of 0 to15, the actual priority assigned to the switch is: (priority-multiplier) x 16.

Examples

Setting the port priority to 8 on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree port-priority 8
```

Setting the port priority to the default on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree port-priority
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree port-type

```
spanning-tree port-type {admin-edge|admin-network}
no spanning-tree port-type [admin-edge|admin-network]
```

Description

Sets the STP port type for the interface.

Port types include: admin-edge and admin-network.

The **no** form of the command sets the port type to the default of admin-network.

Parameter	Description
admin-edge	Specifies the port type as administrative edge. During spanning tree establishment, ports with admin-edge enabled transition immediately to the forwarding state.
admin-network	Specifies the port type as administrative network. When this option is selected, the port looks for BPDUs for the first 3 seconds. If there are none, the port is classified as an edge port and immediately starts forwarding packets. If BPDUs are seen on the port, the port is classified as a non-edge port and normal STP operation commences on that port.

Examples

Setting the port type to admin-edge on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree port-type admin-edge
```

Setting the port type to admin-network on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree port-type admin-network
```

Setting the port type to the default of admin-network on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree port-type
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree priority

spanning-tree priority <PRIORITY-MULTIPLIER>
no spanning-tree priority [<PRIORITY-MULTIPLIER>]

Description

Configures the switch (bridge) priority for the designated region in which the switch resides.

The switch compares this priority with the priorities of other switches in the same region to determine the root switch for the region. The lower the priority value, the higher the priority.

The **no** form of this command sets the bridge priority to the default of 8. The default priority value is derived by multiplying 8 by 4096.

Parameter	Description
<PRIORITY-MULTIPLIER>	Specifies the priority as a multiplier. Range: 0 to 15. Default: 8. The priority range for an MSTP switch is 0-61440. However, this command specifies the priority as a multiplier (0 to 15) of 4096. That is, when you specify a priority multiplier value of 0 to 15, the actual priority assigned to the switch is: (priority-multiplier) x 4096. For example, with 2 as the priority-multiplier on a given MSTP switch, the switch priority setting is 8,192.

Usage

Every switch running an instance of MSTP has a Bridge Identifier, which is a unique identifier that helps distinguish this switch from all others. The switch with the lowest Bridge Identifier is elected as the root for the tree. The Bridge Identifier is composed of a configurable priority component (2 bytes) and the bridge's MAC address (6 bytes). You can change the priority component provides flexibility in determining which switch will be the root for the tree, regardless of its MAC address.

Examples

Setting the priority multiplier to 12:

```
switch(config)# spanning-tree priority 12
```


Setting the priority multiplier to the default of 8:

```
switch(config)# no spanning-tree priority
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree root-guard

```
spanning-tree root-guard  
no spanning-tree root-guard
```

Description

Enables the root guard on the interface.

When a port is enabled as root-guard, it cannot be selected as the root port even if it receives superior STP BPDUs. The port is assigned an "alternate" port role and enters a blocking state if it receives superior MSTP BPDUs.

A superior BPDU contains both "better" information on the root bridge and path cost to the root bridge, which would normally replace the current root bridge selection.

The **no** form of the command sets the root guard status to the default of disabled on the interface.

Examples

Enabling the root guard on interface **1/1/1**:

```
switch(config)# interface 1/1/1  
switch(config-if)# spanning-tree root-guard
```

Disabling root guard on interface **1/1/1**:

```
switch(config)# interface 1/1/1  
switch(config-if)# no spanning-tree root-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree rpvst-filter

spanning-tree rpvst-filter
no spanning-tree rpvst-filter

Description

Enables the RPVST filter for the interface. This command is only applicable to MSTP mode. It is not applicable to RPVST+ mode.

When the RPVST filter is enabled, the ingressing RPVST proprietary BPDUs are dropped after copying to CPU whereas the standard IEEE RPVST BPDUs are still allowed. This helps in preventing the flooding of RPVST proprietary BPDUs under an MSTP-RPVST interop environment.



If the neighboring switch is running RPVST then this pair of switches will not converge as RPVST BPDUs will not reach them.

If enabling RPVST filter causes a high traffic load, shutdown the port and reconfigure the BPDU filter with the CLI command: **no spanning tree rpvst-filter**.

RPVST filter is disabled by default.

Example

Enabling the RPVST filter on interface 1/1/1:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree rpvst-filter
```

Disabling RPVST filter on interface 1/1/1:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree rpvst-filter
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree rpvst-guard

spanning-tree rpvst-guard
no spanning-tree rpvst-guard

Description

Enables RPVST guard on the switch interface. This command is only applicable to MSTP mode. It is not applicable to RPVST+ mode.

When RPVST guard is enabled on an interface, it will disable that interface if RPVST BPDUs are received on it.

The **no** form of the command sets the RPVST guard status to the default of disabled on the interface.

Example

Enabling RPVST guard on interface 1/1/1:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree rpvst-guard
```

Disabling RPVST guard on interface 1/1/1:

```
switch# configure terminal
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree rpvst-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree tcn-guard

```
spanning-tree tcn-guard
no spanning-tree tcn-guard
```

Description

Enables the TCN (Topology Change Notification) guard in the interface. When enabled for a port, the port stops propagating received topology change notifications and topology changes to other ports. The **no** form of the command sets the TCN guard status to the default of disabled on the interface.

Examples

Enabling TCN guard on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree tcn-guard
```

Disabling TCN guard on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no spanning-tree tcn-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree transmit-hold-count

```
spanning-tree transmit-hold-count <COUNT>
no spanning-tree transmit-hold-count [<COUNT>]
```

Description

Sets the maximum number of BPDUs per second that the switch can send from an interface. The **no** form of this command sets the transmit-hold-count to the default of 6.

Parameter	Description
<COUNT>	Specifies the number of BPDUs that can be sent per second. Range: 1 to 10. Default: 6.

Examples

Setting the transmit-hold-count to 5:

```
switch(config)# spanning-tree transmit-hold-count 5
```

Setting the transmit-hold-count to the default of 6:

```
switch(config)# no spanning-tree transmit-hold-count
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree trap

```
spanning-tree trap {new-root|topology-change [instance <INSTANCE-ID>] |
    errant-bpdu | root-guard-inconsistency | loop-guard-inconsistency}
no spanning-tree trap {new-root|topology-change [instance <INSTANCE-ID>] |
    errant-bpdu | root-guard-inconsistency | loop-guard-inconsistency}
```

Description

Enables SNMP traps for new root, topology change event, errant-bpdu received event, root-guard inconsistency, and loop-guard inconsistency notifications. It is disabled by default.

The **no** form of this command disables the notifications for SNMP traps.

Parameter	Description
new-root	Enabling SNMP notification when a new root is elected on any MST instance on the switch.
topology-change	Enabling SNMP notification when a topology change event occurs in the specified MST instance on the switch.
<INSTANCE-ID>	Specifies the instance ID for the topology change trap. Range: 0 to 4094.
errant-bpdu	Enabling SNMP notification when an errant bpdu is received by any MST instance on the switch.
root-guard-inconsistency	Enabling SNMP notification when the root-guard finds the port inconsistent for any MST instance on the switch.
loop-guard-inconsistency	Enabling SNMP notification when the loop-guard finds the port inconsistent for any MST instance on the switch.

Examples

Enabling the notifications for the SNMP traps:

```
switch(config)# spanning-tree trap
  new-root          Enable notifications which are sent when a new root is
  elected
  topology-change   Enable notifications which are sent when a topology
  change occurs
  errant-bpdu       Enable notifications which are sent when an errant
  bpdu is received
  root-guard-inconsistency Enable notifications which are sent when root guard
  inconsistency occurs
  loop-guard-inconsistency Enable notifications which are sent when loop guard
  inconsistency occurs
switch(config)# spanning-tree trap new-root
<cr>
switch(config)# spanning-tree trap topology-change
  instance Enable topology change notification for the specified MST instance id.
switch(config)# spanning-tree trap topology-change instance
  <0-4094> Enable topology change information on the specified instance id.
switch(config)# spanning-tree trap topology-change instance 1
<cr>
switch(config)# spanning-tree trap errant-bpdu
<cr>
switch(config)# spanning-tree trap root-guard-inconsistency
<cr>
switch(config)# spanning-tree trap loop-guard-inconsistency
<cr>
```

Disabling the notifications for the SNMP traps:

```
switch(config)# no spanning-tree trap
  new-root          Disable notifications which are sent when a new root
  is elected
  topology-change   Disable notifications which are sent when a topology
```

```

change occurs
  errant-bpdu          Disable notifications which are sent when an errant
  bpdu is received
  root-guard-inconsistency Disable notifications which are sent when root guard
  inconsistency occurs
  loop-guard-inconsistency Disable notifications which are sent when loop guard
  inconsistency occurs
switch(config)# no spanning-tree trap new-root
<cr>
switch(config)# no spanning-tree trap topology-change
  instance Disable topology change notification for the specified MST instance
switch(config)# no spanning-tree trap topology-change instance
  <0-4094> Disable topology change information on the specified instance id
switch(config)# no spanning-tree trap topology-change instance 1
<cr>
switch(config)# no spanning-tree trap errant-bpdu
<cr>
switch(config)# no spanning-tree trap root-guard-inconsistency
<cr>
switch(config)# no spanning-tree trap loop-guard-inconsistency
<cr>

```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

clear ip mroute

```
clear ip mroute
  all-vrfs
  group-prefix <group-prefix>
  <group-address> [<source-address>]
  <port>
  vrf <vrf-name>
```

Description

Clears the multicast routing information for a specified VRF or all VRFs. If you do not include VRF information in these commands, the **clear ip mroute** commands clear the **default** VRF.

Parameter	Description
all-vrfs	Clears multicast routing for all VRFs.
<group-address>	Clears the multicast routing information for the group address in the specified VRF or all VRFs. If the command does not include VRF information, it clears routing information for the group address in the default VRF.
<source-address>	Clears multicast routing information for the group and source addresses in the specified VRF or all VRFs. If the command does not include VRF information, it clears routing information for the group and source addresses in the default VRF.
group-prefix <group-prefix>	Clears the multicast routing information for the group prefix in the specified VRF or all VRFs. The group prefix must be in the format A.B.C.D/length . If the command does not include VRF information, it clears routing information for the group address in the default VRF.
<port>	Clears the multicast routing information for the port in the specified VRF or all VRFs. If the command does not include VRF information, it clears routing information for the port in the default VRF.
vrf <VRF-NAME>	Clears multicast routing information for a specific VRF.

Examples

Clears multicast routing information for the default VRF.

```
switch# clear ip mroute
```

Clears multicast routing information the group address **225.1.1.1** for the VRF **Lab2**.


```
switch# clear ip mroute 225.1.1.1 vrf Lab2
```

Clears multicast routing information the group address **225.1.1.1** and source address 192.0.2.6 for all VRFs

```
switch# clear ip mroute 225.1.1.1 192.0.2.6 all-vrfs
```

Clears multicast routing information for the port **VLAN10** on the **Default** VRF.

```
clear ip mroute vlan10
```

Clears multicast routing information for the port **VLAN10** for the group address **225.1.1.1** and source address **192.0.2.6** for the VRF **Lab3**.

```
switch# clear ip mroute vlan20 225.1.1.1 192.0.2.6 Lab3
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced on 5420 Switch series.
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip pim-sparse datapath-auto-include

```
ip pim-sparse datapath-auto-include  
no ip pim-sparse datapath-auto-include
```

Description

Enables the router to forward multicast data received on the VXLAN L3VNI fabric to this interface, regardless of whether a multicast join was received on this interface or not. This allows the interface to be in the same multicast data path state on both the VSX peers.

This command must be enabled on the VSX VXLAN routers to support multicast receivers over ROP or P2P SVI extensions. This command can be enabled on a transit L3 peering between VSX peers. This command is optional when the uplink is an MCLAG SVI.

The **no** form of the command disables forwarding of multicast data on the interface.



- An IP address must be configured on the interface and `pim-sparse` must be enabled.
- This command must be enabled only on one interface per VRF.

PIM enabled VXLAN VTEPs can be extended to other routers that can be connected to sources or clients. The following types of L3 or L2 extensions are supported:

- L2 VSX LAG: Upstream or downstream routers are connected using L2 VSX LAG links.
- L3 VSX LAG: Upstream or downstream routers are connected using L3 VSX LAG links.
- ROP extension: L3 extension for sources or clients using ROPs is supported.
- Point-to-point SVI extension: L3 extension for sources or clients using point-to-point SVIs is supported.

If the source is connected using ROP or P2P SVIs, it is recommended to have an additional L3 link per VRF between the VSX devices for upstream redundancy. If the L3 link is an SVI, it is recommended to not add an ISL port in that VLAN.

Parameter	Description
<code>datapath-auto-include</code>	Includes the interface for multicast data forwarding.

Examples

Configuring interface 40.0.0.4/24 of the router to forward multicast data:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-sparse enable
switch(config-if-vlan)# ip pim-sparse datapath-auto-include
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-if-vlan</code>	Administrators or local user group members with execution rights for this command.

ip pim-sparse vsx-virtual-neighbor

```
ip pim-sparse vsx-virtual-neighbor
```

```
no ip pim-sparse vsx-virtual-neighbor
```

Description

Once configured, the router processes IGMP/MLD and PIM joins received on this interface regardless of its DR or Prime Neighbor role. The command must be enabled for VSX VXLAN leaf switches for both L2 and L3 extensions. This allows for the interface to be in the same multicast data path state on both the VSX peers.

The **no** form of the command disables the vsx-virtual-neighbor on the interface.



This command is applicable for normal SVI interfaces and L2 VNI mapped SVI interfaces. It is valid for VXLAN-enabled VLANs only and has no effect on non-VXLAN-enabled VLANs.

Examples

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-sparse enable
switch(config-if-vlan)# ip pim-sparse vsx-virtual-neighbor
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

datapath-auto-include

```
ipv6 pim6-sparse datapath-auto-include
no ipv6 pim6-sparse datapath-auto-include
```

Description

Enables the router to forward multicast data received on the VXLAN L3VNI fabric to this interface, regardless of whether a multicast join was received on this interface or not. This allows the interface to be in the same multicast data path state on both the VSX peers.

This command must be enabled on the VSX VXLAN routers to support multicast receivers over ROP or P2P SVI extensions. This command can be enabled on a transit L3 peering between VSX peers. This command should not be enabled when the uplink is an MCLAG SVI.

The **no** form of the command disables forwarding of multicast data on the interface.



- An IP address must be configured on the interface and `pim-sparse` must be enabled.
- This command must be enabled only on one interface per VRF.

PIM enabled VXLAN VTEPs can be extended to other routers that can be connected to sources or clients. The following types of L3 or L2 extensions are supported:

- L2 VSX LAG: Upstream or downstream routers are connected using L2 VSX LAG links.
- L3 VSX LAG: Upstream or downstream routers are connected using L3 VSX LAG links.
- ROP extension: L3 extension for sources or clients using ROPs is supported.
- Point-to-point SVI extension: L3 extension for sources or clients using point-to-point SVIs is supported.

If the source is connected using ROP or P2P SVIs, it is recommended to have an additional L3 link per VRF between the VSX devices for upstream redundancy. If the L3 link is an SVI, it is recommended to not add an ISL port in that VLAN.

Parameter	Description
<code>datapath-auto-include</code>	Includes the interface for multicast data forwarding.

Examples

Configuring interface 40.0.0.4/24 of the router to forward multicast data:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 40:40::4/64
switch(config-if-vlan)# ipv6 pim6-sparse enable
switch(config-if-vlan)# ipv6 pim6-sparse datapath-auto-include
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-if-vlan</code>	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse vsx-virtual-neighbor

`ipv6 pim6-sparse vsx-virtual-neighbor`

```
no ipv6 pim6-sparse vsx-virtual-neighbor
```

Description

Once configured, the router processes IGMP/MLD and PIM joins received on this interface regardless of its DR or Prime Neighbor role. The command must be enabled for VSX VXLAN leaf switches for both L2 and L3 extensions. This allows for the interface to be in the same multicast data path state on both the VSX peers.

The **no** form of the command disables the vsx-virtual-neighbor on the interface.



This command is applicable for normal SVI interfaces and L2 VNI mapped SVI interfaces. It is valid for VXLAN-enabled VLANs only and has no effect on non-VXLAN-enabled VLANs.

Examples

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 40:40::4/64
switch(config-if-vlan)# ipv6 pim6-sparse enable
switch(config-if-vlan)# ipv6 pim6-sparse vsx-virtual-neighbor
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

register-source

```
register-source <INTERFACE-NAME>
no register-source <INTERFACE-NAME>
```

Description

Specifies the source interface to be used for PIM registration in the case of VXLAN anycast interfaces. When the PIM enabled anycast VLAN is directly connected to a multicast source, **register-source** is used to send registration messages to the RP and this interface receives the register-stop messages from the RP.

The **no** form of this command removes the register source configuration.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the name of the interface to use.

Usage

- This is a global configuration under router-pim configuration and is required in Symmetric IRB with anycast IP address configuration.
- This configuration is required in the source connected switch only when the PIM-DR and RP are in two different switches.
- Without this configuration, there will be traffic loss as the registration sequence will not be successful. It is mandatory to have this source interface configured with a non-anycast IP address which is unique to the VTEP, and with PIM enabled.

Examples

Configuring the source interface for PIM registrations:

```
switch# config
switch(config)# router pim vrf vrf1
switch(config-pim)# register-source loopback1
```

Removing the **register-source** configuration:

```
switch(config-pim)# no register-source loopback1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

show ip mroute

```
show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows all PIM neighbors information.
vrf <VRF-NAME>	Shows PIM neighbor information for a specific VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Multicast route with L3VNI in Incoming Interface List:

```
switch# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address          : 225.1.1.1
Source Address         : 80.1.1.11
Neighbor               : 1.1.1.1
Incoming interface     : vni2
Outgoing Interface List :
Interface              State
-----
vlan10                 forwarding

switch# show ip mroute 225.1.1.1 80.1.1.11 all-vrfs
IP Multicast Route Entries

VRF : red

Group Address          : 225.1.1.1
Source Address         : 80.1.1.11
Neighbor               : 1.1.1.1
Incoming interface     : vni2
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : BGP
Metric                 : 0
Metric Pref             : 200
Uptime (HH:MM:SS)      : 00:07:23
Downstream Interface
Interface              State
-----
vni2                   forwarding
vni2                   forwarding
```

Multicast route with L3VNI in Outgoing Interface List:

```
switch# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1
```

```

Group Address      : 225.1.1.1
Source Address     : 80.1.1.11
Neighbor          :
Incoming interface : vlan20
Outgoing Interface List :
Interface          State
-----
vni2               forwarding

switch# show ip mroute 225.1.1.1 80.1.1.11 vrf red

IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address      : 225.1.1.1
Source Address     : 80.1.1.11
Neighbor          :
Incoming interface : vlan20
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : connected
Metric            : 0
Metric Pref       : 0
Uptime (HH:MM:SS) : 00:06:32
Downstream Interface
Interface          State
-----
vni2               forwarding

```

Detailed multicast route that displays the individual VTEPs to which the packet is forwarded:

```

switch# show ip mroute 239.2.2.2 100.2.1.4 vrf red detail

VRF : red

Group Address      : 239.2.2.2
Source Address     : 100.2.1.4
SSM Mroute        : False
Neighbor          : 20.20.20.2
Incoming interface : 1/1/2
Unicast Routing Protocol: OSPF
Metric            : 200
Metric Pref       : 110
Downstream Interface
Interface          State      Proxy-DR      VTEPS
-----
vni1000           forwarding  false        3.3.3.3

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim neighbor

```
show ip pim neighbor [<IP-ADDR>] [all-vrfs | vrf <VRF-NAME>]
show ip pim neighbor [<BRIEF>] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays the information about PIM interfaces currently configured in the router for the given VRF. If VRF is not given, it displays for default VRF.

Parameter	Description
<IP-ADDR>	Shows PIM neighbor information.
<BRIEF>	Shows brief PIM neighbor information.
all-vrfs	Shows all PIM neighbors information
vrf <VRF-NAME>	Shows PIM neighbor information for a specific VRF.

Examples

Show information for all VRFs:

```
switch# show ip pim neighbor all-vrfs

PIM Neighbor

VRF                               : Test_1
Total number of neighbors       : 2

IP Address                       : 100.1.1.252
Interface                       : vlan100
Up Time (HH:MM:SS)              : 00:44:38
Expire Time (HH:MM:SS)         : 00:01:32
DR Priority                     : 1
Hold Time (HH:MM:SS)           : 00:01:45

IP Address                       : 172.1.1.1
Interface                       : vni1000
Up Time (HH:MM:SS)              : 00:44:35
Expire Time (HH:MM:SS)         : 00:03:25
DR Priority                     : 1
Hold Time (HH:MM:SS)           : 00:03:30
```

PIM supports both IPv4 and IPv6 as underlay VTEP IP addresses. In deployments with an IPv6 underlay, PIM forms an auto-generated link-local address to exchange control packets and forms a PIM neighborhood over an L3VNI interface with other VTEPs. The auto generated IP will be a link local IP in case of overlay IPv6.

The following example displays L3VNI neighbors for an IPv6 underlay tunnel with an IPv4 overlay.

```

switch# show ip pim neighbor all-vrfs
PIM Neighbor
VRF : Test_1
Total number of neighbors : 1
IP Address : 169.254.125.33
Interface : vni1000
Up Time (HH:MM:SS) : 00:44:35
Expire Time (HH:MM:SS) : 00:03:25
DR Priority : 1
Hold Time (HH:MM:SS) : 00:03:30

```

In deployments with an IPv4 overlay, multicast route entries with an incoming L3VNI interface will have a neighbor ip address that is an auto-generated IPv4 address derived from the underlay V6 tunnel address,

```

switch# show ip mroute 230.1.1.1 vrf Test_1 detail
IP Multicast Route Entries
VRF : Test_1
Total number of entries : 1
Group Address : 230.1.1.1
Source Address : 40.40.1.100
Neighbor : 169.254.125.33
Incoming interface : vni1000
Unicast Routing Protocol : BGP
Metric : 0
Metric Pref : 200
Uptime (HH:MM:SS) : 00:01:45
Downstream Interface
Interface State
-----
vlan20 forwarding

```

Show **brief** information for PIM neighbor:

```

switch# show ip pim neighbor brief
-----
VRF: default Total number of neighbor : 2
-----
Interface Neighbor Uptime Expires DR Hold Time
Secondary Address (IPV4) (HH:MM:SS) (HH:MM:SS) Priority (HH:MM:SS)
-----
1/1/1 40.0.0.5 11:54:21 00:01:31 1000 00:01:45 Nil
1/1/2 50.0.0.5 00:03:23 00:01:23 500 00:01:45 60.0.0.4 ,
70.0.0.4
-----

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute

```
show ipv6 mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows all PIM neighbors information.
vrf <VRF-NAME>	Shows PIM neighbor information for a specific VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing multicast route with L3VNI in Incoming Interface List:

```
switch# show ipv6 mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address      : ff55::100:1
Source Address     : 200:200::100
SSM Mroute        : False
Neighbor          : fe80::5:5:5:5
Uptime            : 00:02:37
State             : route
Incoming interface : vni2
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding
```

```

switch# show ipv6 mroute ff55::100:1 200:200::100 vrf red

IP Multicast Route Entries

VRF : red

Group Address          : ff55::100:1
Source Address         : 200:200::100
Neighbor               :
Incoming interface     : vni2
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : BGP
Metric                 : 0
Metric Pref            : 200
Uptime (HH:MM:SS)      : 00:10:24

```

Showing multicast route with L3VNI in Outgoing Interface List:

```

switch# show ipv6 mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address          : ff55::100:1
Source Address         : 200:200::100
Neighbor               :
Uptime                 : 00:06:38
State                  : route
Incoming interface     : vlan20
Outgoing Interface List :
Interface              State
-----
vni2                   forwarding

```

```

switch# show ipv6 mroute ff55::100:1 200:200::100 vrf red
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address          : ff55::100:1
Source Address         : 200:200::100
Neighbor               :
Incoming interface     : vlan20
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : connected
Metric                 : 0
Metric Pref            : 0
Uptime (HH:MM:SS)      : 00:06:38
Downstream Interface
Interface              State
-----
vni2                   forwarding

```

Showing detailed multicast route that displays the individual VTEPs to which the packet is forwarded:

```
switch# show ipv6 mroute all-vrfs ff55::100:1 200:200::100 vrf red detail
```

```
VRF : red
Total number of entries : 1

Group Address      : ff55::100:1
Source Address     : 200:200::100
SSM Mroute        : False
Neighbor          :
Incoming Interface : vlan20
Unicast Routing Protocol: connected
Metric            : 0
Metric Pref       : 0
Downstream Interface
Interface      State      Proxy-DR      VTEPs
-----
vni2          forwarding  false        3.3.3.3
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface vlan

```
show ipv6 pim6 interface vlan <vlan name>
```

Description

Displays the IPV6 information about PIM6 interfaces currently configured in the router for the given VLAN. If the VLAN name is not specified, the output of this command displays information for the default VLAN.

Parameter	Description
vlan <vlan name>	Specifies the VLAN.

Examples

Showing the IPV6 information about PIM6 interfaces currently configured in the router for VLAN 301:

```

switch(config)# show ipv6 pim6 interface vlan301
Interface                : vlan301
Neighbor count           : 1
IPv6 Address             : fe80::5480:2881:2dfc:b200/64
Mode                     : sparse
Designated Router        : fe80::5480:2881:2dfc:b200
Proxy DR                 : false
Hello Interval (sec)     : 30
Hello Delay (sec)        : 5
Override Interval (msec) : 2500
Propagation Delay (msec) : 500
Operational DR Priority   : 100
Neighbor Timeout         : 82
VSX Virtual Neighbor     : true
Datapath Auto Include    : true
Lan Prune Delay          : Yes
Configured DR Priority    : 100

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

```

switch (config-if-vlan)# show traffic-insight test monitor-type dns-average-
latency
mon2 error-statistics
Type                : dns-average-latency
Start time for error monitoring : 10/10/2022 04:12:13.923691 UTC
End time for error monitoring   : 10/10/2022 04:17:13.964505 UTC

client_mac      dns_server_ip  number_of_  dns_name  dns_server  dns_format
                dns_server_ip  dns_failures _errors   _failures   _errors
-----
--
aa:aa:aa:aa:aa:aa  172.0.0.1      200         50        100         50
bb:bb:bb:bb:bb:bb  172.1.1.1      50          10         20          20
cc:cc:cc:cc:cc:cc  172.2.2.2     150         75         25          50

```

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

show ipv6 pim6 neighbor

show ipv6 pim6 neighbor [<IP-ADDR>] [all-vrfs | vrf <VRF-NAME>]

Description

Displays the information about PIM interfaces currently configured in the router for the given VRF. If VRF is not given, it displays for default VRF.



The overlay IPv6 address of the LRVNI is an autogenerated link local IP that is derived by PIM using the VXLAN source IP.

Parameter	Description
<IP-ADDR>	Shows PIM neighbor information.
all-vrfs	Shows all PIM neighbors information
vrf <VRF-NAME>	Shows PIM neighbor information for a specific VRF.

Examples

Show information for all VRFs:

```
switch# show ipv6 pim6 neighbor all-vrfs

PIM Neighbor

VRF                               : red
Total number of neighbors       : 2

IPv6 Address                     : fe80::5:5:5:5
Interface                       : vni10000
Up Time (HH:MM:SS)              : 06:57:307
Expire Time (HH:MM:SS)          : 00:03:26
DR Priority                      : 1
Hold Time (HH:MM:SS)            : 00:03:30

IPv6 Address                     : fe80::3281:c780:a5c:18c0
Interface                       : vlan10
Up Time (HH:MM:SS)              : 00:01:46
Expire Time (HH:MM:SS)          : 00:01:29
DR Priority                      : 1
Hold Time (HH:MM:SS)            : 00:01:45
Secondary IP Addresses           : 100:100::3
```

PIM supports both IPv4 and IPv6 as underlay VTEP IP addresses. If the outgoing interface is a L3VNI, the forwarded VTEP IP address will be displayed as the actual IPv6 underlay tunnel source IP address.

```
switch# show ipv6 mroute 230.1.1.1 vrf Test_1 detail
IP Multicast Route Entries
VRF : Test_1
Total number of entries : 1
Group Address             : 230.1.1.1
Source Address            : 40.40.1.100
Neighbor                  : 100.100.1.1
Incoming interface        : 1/1/6
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol  : BGP
Metric                   : 0
Metric Pref               : 20
Uptime (HH:MM:SS)        : 00:02:06
Downstream Interface
Interface      State      Vsteps
-----
-----
```

vn1000	forwarding	5::5

The following example displays L3VNI neighbors for an underlay IPv6 tunnel with an IPv6 overlay

```
switch# show ipv6 pim6 neighbor all-vrfs
PIM Neighbor
VRF : Test_1
Total number of neighbors : 1
IP Address : fe80::165:72:119
Interface : vn1000
Up Time (HH:MM:SS) : 00:40:38
Expire Time (HH:MM:SS) : 00:01:32
DR Priority : 1
Hold Time (HH:MM:SS) : 00:01:45
```

In deployments with an IPv6 overlay, multicast route entries with an incoming L3VNI interface will have a neighbor IP that is an auto-generated IPv6 address derived from the IPv6 underlay tunnel. This example displays multicast routes for an IPv6 underlay tunnel with an IPv6 overlay.

```
switch# show ipv6 mroute ff55::1 vrf Test_1 detail
IP Multicast Route Entries
VRF : Test_1
Total number of entries : 1
Group Address : ff55::1
Source Address : 40:40::100
Neighbor : fe80::165:72:119
Incoming interface : vn1000
Unicast Routing Protocol : BGP
Metric : 0
Metric Pref : 200
Uptime (HH:MM:SS) : 00:01:45
Downstream Interface
Interface State
-----
vlan20 forwarding
```

If the outgoing interface is L3VNI, the forwarded VTEP IP address will be displayed as the actual underlay IPv6 tunnel source IP.

```
switch# show ipv6 mroute ff55::1 vrf Test_1 detail
IP Multicast Route Entries
VRF : Test_1
Total number of entries : 1
Source Address : 40:40::100
Neighbor : fe80::f860:f001:4057:6900
Incoming interface : 1/1/6
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : BGP
Metric : 0
Metric Pref : 20
Uptime (HH:MM:SS) : 00:02:06
Downstream Interface
Interface State Vteps
-----
vn1000 forwarding 5::5
Group Address : ff55::1
```




For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip multicast multi-fabric identifier

```
ip multicast multi-fabric identifier-value <IDENTIFIER VALUE> <cr>  
no ip multicast multi-fabric <IDENTIFIER-VALUE>
```

Description

Configures multicast fabric identifier (MFID) that uniquely represents the fabric/site to which this leaf router belongs. Shown in the PIM hello option field, this command is used by the border router to associate the neighbor to the fabric MFID. This command is applicable to all the regular leaf routers and not applicable at the shared border router.

The **no** form of the command disables forwarding of multicast data on the interface.

The same MFID value must be configured on all leaf routers belonging to the same fabric. However, the same MFID value cannot be reused between fabrics attached to the same border.

Configuration of an Identifier is optional on the VTEPs. If there is no manually configured Identifier, it will automatically use and announce the local AS Number as Identifier.

Parameter	Description
<IDENTIFIER VALUE>	Configures the given value as MFID

Examples

Configuring **ip multicast multi-fabric identifier-value** command:

```
switch(config)#  
switch(config)# ip multicast multi-fabric identifier <identifier-value> <cr>  
switch(config)# no ip multicast multi-fabric identifier <identifier-value> <cr>  
switch(config)#  
switch(config)# ipv6 multicast multi-fabric identifier <identifier-value> <cr>  
switch(config)# no ipv6 multicast multi-fabric identifier <identifier-value> <cr>
```

Configuring MFID value of 1001 on two VTEPs using the same fabric:

```
On VTEP1:
vtep1(config)#
vtep1(config)# ip multicast multi-fabric identifier 1001 <cr>
```

```
On VTEP2:
vtep2(config)#
vtep2(config)# ip multicast multi-fabric identifier 1001 <cr>
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

Multicast datapath commands for IPv4

show ip multicast bridging datapath

```
show ip multicast bridging datapath {group <GROUP-IP> {source <SOURCE-IP>
{vlan <VLAN-ID>}}}[vrf <VRF_NAME>] [vsx-peer]
```

Description

Displays the multicast bridge control forwarding entries on a device including replication details and hardware programming status. Displays bridging datapath details for the specified multicast flow (the group, source, VLAN, and VRF).

Parameter	Description
group <GROUP-IP>	Specifies a group IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Shows bridging datapath details for the specified group.
source <SOURCE-IP>	Specifies a source IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Shows bridging datapath details for the specified source.
vlan <VLAN-ID>	Specifies a VLAN. Values: 1-4094. Shows bridging datapath details for the specified VLAN.
vrf <VRF-NAME>	Specifies a VRF. Shows datapath information for groups joined in the specified VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

A multicast bridge control forwarding table comprises of the IP multicast destination address, source address and its association with a list of ports on which the multicast packets are replicated in a Layer 2 domain. The switch floods/ replicates the multicast packet on these ports by matching the multicast destination address, source address, and the virtual local network identifier (VLAN ID). The **show ip multicast bridging datapath** command displays the multicast bridge control forwarding entries on a device including replication details and hardware programming status.

Examples

Showing detailed bridging datapath information for the specified multicast flow:

```
switch# show ip multicast bridging datapath group 232.1.1.10 source 100.100.1.10
vlan 10
Multicast Bridging Datapath Details
VRF                               : default
Source                           : 100.100.1.10/32
Group                            : 232.1.1.10/32
Replication Group Index          : 70
Hardware Status                  : active
Error Code                       : None
Retries for programming          : 0
Vlan                             : VLAN10
State                            : forwarding

VNI                               : vni1000
State                             : operational
Replication Details:
Tunnel Endpoints                 State
-----
2.2.2.2                         operational
4.4.4.4                         operational
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast routing datapath

```
show ip multicast routing datapath {group <GROUP-IP> {source <SOURCE-IP>
{port <INCOMING-PORT>}}}[vrf <VRF_NAME>] [vsx-peer]
```

Description

Displays the multicast Layer 3 forwarding entries with replication details and hardware programming status. Displays routing datapath details for the specified multicast flow (group, source, incoming port, and VRF).

Parameter	Description
<code>group <GROUP-IP></code>	Specifies a group IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Shows datapath details for the specified group.
<code>source <SOURCE-IP></code>	Specifies a source IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Shows datapath details for the specified source.
<code>port <INCOMING-PORT></code>	Specifies the incoming port. Shows datapath details for the specified port.
<code>vrf <VRF-NAME></code>	Specifies a VRF. Shows datapath information for the specified VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

A multicast routing protocol such as PIM populates the multicast Layer 3 forwarding table and forwards multicast traffic to clients throughout the network. A multicast forwarding table comprises of the IP multicast destination address, source address, interface on which the traffic is received, and the list of interfaces on which multicast traffic is replicated. The **show ip multicast routing datapath** command displays the multicast Layer 3 forwarding entries with replication details and hardware programming status.

Examples

Showing detailed routing datapath information for the specified multicast flow:

```
switch# show ip multicast routing datapath group 225.20.0.1 source 20.0.0.2 port
vlan20
Multicast Routing Datapath Details
VRF                : default
Source             : 20.0.0.2/32
Group              : 225.20.0.1/32
Primary Upstream Interface : vlan20
From               : pim_sm
Type               : route
Replication Group Index : 38923
Hardware Status    : active
Error Code         : None
Retries for programming : 0
Upstream Interface : vlan20
    State          : forwarding
    Replication Details:
        L2 Ports      State
        -----
        1/1/4         forwarding
Downstream Interface : vlan30
    State          : forwarding
    Replication Details:
        L2 Ports      State
        -----
```

```
1/1/1          forwarding
Downstream Interface : vlan40
State          : forwarding
Replication Details:
L2 Ports      State
-----
1/1/2          forwarding
1/1/3          forwarding
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Multicast datapath commands for IPv6

show ipv6 multicast bridging datapath

```
show ipv6 multicast bridging datapath {group <GROUP-IP> {source <SOURCE-IP>
{vlan <VLAN-ID>}}}[vrf <VRF_NAME>]]]] [vsx-peer]
```

Description

Displays the multicast bridge control forwarding entries on a device including replication details and hardware programming status. Displays bridging datapath details for the specified multicast flow (the group, source, VLAN, and VRF).

Parameter	Description
group <GROUP-IP>	Specifies a group IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Shows bridging datapath details for the specified group.
source <SOURCE-IP>	Specifies a source IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Shows bridging datapath details for the specified source.
vlan <VLAN-ID>	Specifies a VLAN. Range 1 to 4094. Shows bridging datapath details for groups joined in the specified VLAN.
vrf <VRF-NAME>	Specifies a VRF. Shows bridging datapath information for groups joined in the specified VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

A multicast bridge control forwarding table comprises of the IP multicast destination address, source address and its association with a list of ports on which the multicast packets are replicated in a Layer 2 domain. The switch floods/ replicates the multicast packet on these ports by matching the multicast destination address, source address, and the virtual local network identifier (VLAN ID). The **show ipv6 multicast bridging datapath** command displays the multicast bridge control forwarding entries on a device including replication details and hardware programming status.

Examples

Showing detailed bridging datapath information for the specified multicast flow:

```

switch# show ipv6 multicast bridging datapath group ff03::0 source 1010:22::4 vlan
10
Multicast Bridging Datapath Details
VRF                               : default
Source                           : 1010:22::4/128
Group                            : ff03::/128
Replication Group Index          : 70
Hardware Status                   : active
Error Code                       : None
Retries for programming          : 0
Vlan                             : VLAN10
    State                         : forwarding
    Replication Details:
    L2 Ports                      State
    -----
    1/1/6                        forwarding
    1/1/7                        forwarding
VNI                               : vni1000
    State                         : operational
    Replication Details:
    Tunnel Endpoints              State
    -----
    2.2.2.2                      operational
    4.4.4.4                      operational

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 multicast routing datapath

```

show ipv6 multicast routing datapath {group <GROUP-IP> {source <SOURCE-IP>
{port <INCOMING-PORT>}}} [vrf <VRF_NAME>] [vsx-peer]

```

Description

Displays the multicast Layer 3 forwarding entries with replication details and hardware programming status. Displays routing datapath details for the specified multicast flow (group, source, incoming port, and VRF).

Parameter	Description
<code>group <GROUP-IP></code>	Specifies a group IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Shows datapath details for the specified group.
<code>source <SOURCE-IP></code>	Specifies a source IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. Shows datapath details for the specified source.
<code>port <INCOMING-PORT></code>	Specifies the incoming port. Shows datapath details for the specified port.
<code>vrf <VRF-NAME></code>	Specifies a VRF. Shows datapath information for groups joined in the specified VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

A multicast routing protocol such as PIM populates the multicast Layer 3 forwarding table and forwards multicast traffic to clients throughout the network. A multicast forwarding table comprises of the IP multicast destination address, source address, interface on which the traffic is received, and the list of interfaces on which multicast traffic is replicated. The **show ipv6 multicast routing datapath** command displays the multicast Layer 3 forwarding entries with replication details and hardware programming status.

Examples

Showing detailed routing datapath information for the specified multicast flow:

```
switch# show ip multicast routing datapath group 225.20.0.1 source 20.0.0.2 port
vlan20
Multicast Routing Datapath Details
VRF                : default
Source             : 20.0.0.2/32
Group              : 225.20.0.1/32
Primary Upstream Interface : vlan20
From               : pim_sm
Type              : route
Replication Group Index : 38923
Hardware Status    : active
Error Code         : None
Retries for programming : 0
Upstream Interface : vlan20
    State          : forwarding
    Replication Details:
    L2 Ports       State
    -----
    1/1/4          forwarding
Downstream Interface : vlan30
    State           : forwarding
```

```

Replication Details:
L2 Ports          State
-----
1/1/1             forwarding
Downstream Interface : vlan40
State              : forwarding
Replication Details:
L2 Ports          State
-----
1/1/2             forwarding
1/1/3             forwarding

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip multicast-static-route

```
ip multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> [<OUTGOING-INTERFACE-NAME>] vrf <VRF-NAME>
no ip multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> [<OUTGOING-INTERFACE-NAME>] vrf <VRF-NAME>
```

Description

Configures a multicast static route for (source, group) on an incoming interface with outgoing interface (s) not involving L3VNI. If a vrf is not specified, default vrf is used.

The **no** form of this command removes the configuration.

Parameter	Description
<INCOMING-INTERFACE-NAME>	Specifies the multicast stream incoming interface name.
<SOURCE-ADDRESS>	Selects the IPv4 source address.
<ANY>	Selects any source address.
<GROUP-ADDRESS>	Specifies the IPv4 multicast group address.
<OUTGOING-INTERFACE-NAME>	Specifies the outgoing interface name.
vrf <VRF-NAME>	Configures the specified VRF. The default is default vrf.

Usage

If the incoming interface is attached to different vrf than the vrf spcified in the multicast static route command, route will be made inactive. If the vrf mismatch occurs for the outgoing interface, that particular outgoing interface will be made inactive. If no outgoing interface is specified, the multicast traffic is not routed and is bridged on the interface (SVI) on which the traffic is received.

Examples

Configuring Multicast Static Route with a outgoing interface:

```
switch(config)# ip multicast-static-route vlan10 10.10.1.2 239.255.255.250 vlan20
```

Removing the configured Multicast Static Route with a outgoing interface:

```
switch(config)# no ip multicast-static-route vlan10 10.10.1.2 239.255.255.250  
vlan20
```

Configuring Multicast Static Route without an outgoing interface to bridge traffic only in incoming interface in default vrf:

```
switch(config)# ip multicast-static-route vlan30 30.30.1.2 239.255.255.250
```

Removing the configured Multicast Static Route without an outgoing interface to bridge traffic only in incoming interface in default vrf:

```
switch(config)# no ip multicast-static-route vlan30 30.30.1.2 239.255.255.250
```

Configuring Multicast Static Route without an outgoing interface to bridge traffic only in incoming interface in non-default vrf:

```
switch(config)# ipv6 multicast-static-route vlan30 30.30.1.2 239.255.255.250 vrf  
red
```

Removing the configured Multicast Static Route without an outgoing interface to bridge traffic only in incoming interface in non-default vrf:

```
switch(config)# ipv6 multicast-static-route vlan30 30.30.1.2 239.255.255.250 vrf  
red
```

Configuring Multicast Static Route with multiple outgoing interfaces:

```
switch(config)# ip multicast-static-route vlan40 40.40.1.2 239.255.255.250 vlan50  
vrf red  
switch(config)# ip multicast-static-route vlan40 40.40.1.2 239.255.255.250 vlan60  
vrf red  
switch(config)# ip multicast-static-route vlan40 40.40.1.2 239.255.255.250 1/1/1  
vrf red
```

Removing configured Multicast Static Route with multiple outgoing interfaces:

```
switch(config)# no ip multicast-static-route vlan40 40.40.1.2 239.255.255.250  
vlan60 vrf red  
switch(config)# no ip multicast-static-route vlan40 40.40.1.2 239.255.255.250 vrf  
red
```

Configuring Static (*, Group) Multicast Route with multiple outgoing interfaces:

```
switch(config)# ip multicast-static-route vlan50 any 239.255.255.250 vlan70 vrf  
red  
switch(config)# ip multicast-static-route vlan50 any 239.255.255.250 vlan80 vrf  
red
```

Removing configured Static (*, Group) Multicast Route with multiple outgoing interfaces:

```
switch(config)# no ip multicast-static-route vlan50 any 239.255.255.250 vlan70 vrf
red
switch(config)# no ip multicast-static-route vlan50 any 239.255.255.250 vlan80 vrf
red
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip multicast-static-route (l3vni)

```
ip multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> vrf <VRF-NAME>
ip multicast-static-route <VXLAN1> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> [<OUTGOING-INTERFACE-NAME>]vrf <VRF-NAME>
no ip multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> vrf <VRF-NAME>
no ip multicast-static-route {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> [<OUTGOING-INTERFACE-NAME>]vrf <VRF-NAME>
```

Description

Configures a multicast static route for (source, group) involving L3VNI tunnels. If a vrf is not specified, default vrf is used.

The **no** form of this command removes the configuration.

Parameter	Description
<INCOMING-INTERFACE-NAME>	Specifies the multicast stream incoming interface name.
<SOURCE-ADDRESS>	Selects the IPv4 source address.
<ANY>	Selects any source address.
<GROUP-ADDRESS>	Specifies the IPv4 multicast group address.
<OUTGOING-INTERFACE-NAME>	Specifies the outgoing interface name.
vrf <VRF-NAME>	Configures the specified VRF. The default is default vrf.

Usage

If the incoming interface is attached to different vrf than the vrf specified in the multicast static route command, route will be made inactive. If the vrf mismatch occurs for the outgoing interface, that particular outgoing interface will be made inactive.

Examples

Configuring Multicast Static Route with L2VN1 to SVI:

```
switch(config)# ip multicast-static-route vlan10 10.10.1.2 239.255.255.250 vlan30
```

Removing the configured Multicast Static Route with L2VN1 to SVI:

```
switch(config)# no ip multicast-static-route vlan10 10.10.1.2 239.255.255.250  
vlan30
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 multicast-static-route

```
ipvy multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-  
ADDRESS> [<OUTGOING-INTERFACE-NAME>] vrf <VRF-NAME>  
no ipv6 multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-  
ADDRESS> [<OUTGOING-INTERFACE-NAME>] vrf <VRF-NAME>
```

Description

Configures a multicast static route for (source, group) on an incoming interface with outgoing interface (s) not involving L3VNI. If a vrf is not specified, default vrf is used.

The **no** form of this command removes the configuration.

Parameter	Description
<INCOMING-INTERFACE-NAME>	Specifies the multicast stream incoming interface name.
<SOURCE-ADDRESS>	Selects the IPv6 source address.

Parameter	Description
<ANY>	Selects any source address.
<GROUP-ADDRESS>	Specifies the IPv6 multicast group address.
<OUTGOING-INTERFACE-NAME>	Specifies the outgoing interface name.
vrf <VRF-NAME>	Configures the specified VRF. The default is default vrf.

Usage

If the incoming interface is attached to different vrf than the vrf spcified in the multicast static route command, route will be made inactive. If the vrf mismatch occurs for the outgoing interface, that particular outgoing interface will be made inactive.

Examples

Configuring Multicast Static Route with a outgoing interface:

```
switch(config)# ipv6 multicast-static-route vlan10 2001::1 ff02::c vlan20
```

Removing the configured Multicast Static Route with a outgoing interface:

```
switch(config)# no ipv6 multicast-static-route vlan10 2001::1 ff02::c vlan20
```

Configuring Static (*, Group) Multicast Route with multiple outgoing interfaces:

```
switch(config)# ipv6 multicast-static-route vlan50 any ff0e::c vlan70 vrf red
switch(config)# ipv6 multicast-static-route vlan50 any ff0e::c vlan80 vrf red
```

Removing configured Static (*, Group) Multicast Route with multiple outgoing interfaces:

```
switch(config)# no ipv6 multicast-static-route vlan50 any ff0e::c vlan70 vrf red
switch(config)# no ipv6 multicast-static-route vlan50 any ff0e::c vlan80 vrf red
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config	Operators or Administrators or local user group members with

Platforms	Command context	Authority
9300S		execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 multicast-static-route (l3vni)

```

ipv6 multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> vrf <VRF-NAME>
ipv6 multicast-static-route {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> [<OUTGOING-INTERFACE-NAME>]vrf <VRF-NAME>
no ipv6 multicast-static-route <INCOMING-INTERFACE-NAME> {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> vrf <VRF-NAME>
no ipv6 multicast-static-route {<SOURCE-ADDRESS | ANY>} <GROUP-ADDRESS> [<OUTGOING-INTERFACE-NAME>]vrf <VRF-NAME>

```

Description

Configures a multicast static route for (source, group) involving L3VNI tunnels. If a vrf is not specified, default vrf is used.

The **no** form of this command removes the configuration.

Parameter	Description
<INCOMING-INTERFACE-NAME>	Specifies the multicast stream incoming interface name.
<SOURCE-ADDRESS>	Selects the IPv6 source address.
<ANY>	Selects any source address.
<GROUP-ADDRESS>	Specifies the IPv6 multicast group address.
<OUTGOING-INTERFACE-NAME>	Specifies the outgoing interface name.
vrf <VRF-NAME>	Configures the specified VRF. The default is default vrf.

Usage

If the incoming interface is attached to different vrf than the vrf spcified in the multicast static route command, route will be made inactive. If the vrf mismatch occurs for the outgoing interface, that particular outgoing interface will be made inactive.

Examples

Configuring Multicast Static Route with L2VN1 to SVI:

```
switch(config)# ipv6 multicast-static-route vlan10 2001::1 ff02::c vlan30
```

Removing the configured Multicast Static Route with L2VN1 to SVI:


```
switch(config)# no ipv6 multicast-static-route vlan10 2001::1 ff02::c vlan30
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

redistribute static

```
redistribute static  
no redistribute static
```

Description

Exports all static multicast routes configured on a VRF to the corresponding PIM router. The **no** form of this command disables the redistribution.

Usage

Static multicast routes give the flexibility to program a specific path for multicast traffic from the source to the client without having to rely on the underlying protocols to build a multicast route. They can be configured on all the routers in the path or on a specific section of routers. The remaining section of routers can be configured to run the native PIM protocol. In such cases, the static multicast route is exported to PIM domain as PIM joins using this command.

Examples

Configuring redistribute static routes to PIM for IPv4:

```
switch(config)# router pim  
switch(config-pim)# redistribute static
```

Disabling redistribute static routes to PIM for IPv4:

```
switch(config)# router pim  
switch(config-pim)# no redistribute static
```

Configuring redistribute static routes to PIM for IPv4 on vrf red:

```
switch(config)# router pim vrf red  
switch(config-pim)# redistribute static
```

Disabling redistribute static routes to PIM for IPv4 on vrf red:

```
switch(config)# router pim vrf red
switch(config-pim)# no redistribute static
```

Configuring redistribute static routes to PIM for IPv6:

```
switch(config)# router pim6
switch(config-pim)# redistribute static
```

Disabling redistribute static routes to PIM for IPv6:

```
switch(config)# router pim6
switch(config-pim)# no redistribute static
```

Configuring redistribute static routes to PIM for IPv6 on vrf red:

```
switch(config)# router pim6 vrf red
switch(config-pim)# redistribute static
```

Disabling redistribute static routes to PIM for IPv6 on vrf red:

```
switch(config)# router pim6 vrf red
switch(config-pim)# no redistribute static
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config config-pim	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show capacities multicast static route

```
show capacities multicast-static-route
show capacities-status multicast-static route
```

Description

Displays the maximum number of IPv4 and IPv6 static multicast routes that can be configured on the devices.

Examples

Displaying the maximum number of multicast static routes configured on the device:

```

switch# show capacities static-multicast-route
System Capacities: Filter Static Multicast Route
Capacities Name                                     Value
-----
---
Maximum number of IPv4/IPv6 Static multicast nexthops supported      65536
Maximum number of IPv4/IPv6 Static multicast routes supported         4096
Maximum number of IPv4/IPv6 Summarized static multicast routes supported 1024

switch# show capacities-status static-multicast-route
System Capacities Status: Filter Static Multicast Route
Capacities Status Name                                     Value      Maximum
-----
---
Number of IPv4/IPv6 Static multicast nexthops                  10         65536
Number of IPv4/IPv6 Static multicast routes                    33         4096
Number of IPv4/IPv6 Summarized static multicast routes         6          1024

```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast-static-route

show ip multicst-static-route [all vrfs | vrf <VRF-NAME>]

Description

Displays the multicast static route and corresponding summarized route information for the specified VRF. If VRF is not specified, the default VRF is displayed.

Parameter	Description
[all vrfs]	Selects all VRFs to display.
[vrf <VRF-NAME>]	Specifies the VRF to display. The default is default vrf.

Examples

Displaying the multicast static route and corresponding summarized route information for all vrfs:

```

switch# show ip multicast-static-route all-vrfs
VRF : red

```

```

Group Address          : 239.255.255.250
Source Address         : 40.40.40.2
Route type             : Static
Incoming interface     : 1/1/2
Outgoing Interface List :
Interface      State
-----
vlan10         forwarding

VRF : blue

Group Address          : 239.255.255.250
Source Address         : Any
Route type             : Static-Summarized
Incoming interface     : 1/1/3
Outgoing Interface List :
Interface      State
-----
vlan20         forwarding
vlan30         forwarding

```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast-static-route detail

show ip multicst-static-route <GROUP-ADDRESS> {<SOURCE-ADDRESS | ANY>} detail [all vrfs | vrf <VRF-NAME>]

Description

Displays the multicast static route and corresponding summarized route information for the given group address in the given VRF detail. If VRF is not specified, the default VRF is displayed.

Parameter	Description
<GROUP-ADDRESS>	Specifies the group address.
<SOURCE-ADDRESS>	Specifies the source address.
<ANY>	Selects any source address.
[all vrfs]	Selects all VRFs to display.

Parameter	Description
[vrf <VRF-NAME>]	Specifies the VRF to display. The default is default vrf.

Examples

Displaying the multicast static route information for a specific group:

```
switch# show ip multicast-static-route 239.255.255.250 40.40.40.3 detail vrf red

VRF : red

Group Address           : 239.255.255.250
Source Address          : 40.40.40.2
Route type              : Static
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State      Vteps
-----
vni1000        forwarding  2.2.2.2, 3.3.3.3
```

Displaying the multicast static route information for any group on vrf red:

```
switch# show ip multicast-static-route 239.255.255.250 any detail vrf red

VRF : red

Group Address           : 239.255.255.250
Source Address          : Any
Route type              : Static
Incoming interface      : 1/1/2
Outgoing Interface List :

Interface      State      Vteps
-----
vni1000        forwarding  2.2.2.2, 3.3.3.3
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast-static-route (group)

```
show ip multicast-static-route <GROUP-ADDRESS> {<SOURCE-ADDRESS | ANY>} [all vrfs | vrf <VRF-NAME>]
```

Description

Displays the multicast static route and corresponding summarized route information for the given group address in the given VRF briefly. If VRF is not specified, the default VRF is displayed.

Parameter	Description
<GROUP-ADDRESS>	Specifies the group address.
<SOURCE-ADDRESS>	Specifies the source address.
<ANY>	Selects any source address.
[all vrfs]	Selects all VRFs to display.
[vrf <VRF-NAME>]	Specifies the VRF to display. The default is default vrf.

Examples

Displaying the multicast static route information for all vrfs:

```
switch# show ip multicast-static-route 239.255.255.250 all-vrfs

VRF : red

Group Address           : 239.255.255.250
Source Address          : 40.40.40.2
Route type              : Static
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
-----
vlan10         forwarding

VRF : blue

Group Address           : 239.255.255.250
Source Address          : Any
Route type              : Static-summarized
Incoming interface      : 1/1/3
Outgoing Interface List :
Interface      State
-----
vlan20         forwarding
vlan30         forwarding
```

Displaying the multicast static route information for a specific group on vrf red:

```
switch# show ip multicast-static-route 239.255.255.250 40.40.40.4 vrf red

VRF : red

Group Address           : 239.255.255.250
Source Address          : Any
Route type              : Static
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
```

```

-----
vlan10      forwarding

```

Displaying the multicast static route information for a specific group and source :

```

switch# show ip multicast-static-route 239.255.255.250 40.40.40.2 all-vrfs
VRF : red

Group Address      : 239.255.255.250
Source Address     : 40.40.40.2
Route type         : Static
Incoming interface : 1/1/2
Outgoing Interface List :
Interface          State
-----
vlan10             forwarding

VRF : blue

Group Address      : 239.255.255.250
Source Address     : 40.40.40.2
Route type         : Static
Incoming interface : vlan40
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding
vlan30             forwarding

```

Displaying the multicast static route information for a specific group and any source :

```

switch# show ip multicast-static-route 239.255.255.250 any all-vrfs
VRF : red

Group Address      : 239.255.255.250
Source Address     : Any
Route type         : Static-summarized
Incoming interface : 1/1/2
Outgoing Interface List :
Interface          State
-----
vlan10             forwarding

VRF : blue

Group Address      : 239.255.255.250
Source Address     : Any
Route type         : Static-summarized
Incoming interface : vlan40
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding
vlan30             forwarding

```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 multicast-static-route

```
show ipv6 multicast-static-route [all vrfs | vrf <VRF-NAME>]
```

Description

Displays the multicast static route and corresponding summarized route information for the specified VRF. If VRF is not specified, the default VRF is displayed.

Parameter	Description
[all vrfs]	Selects all VRFs to display.
[vrf <VRF-NAME>]	Specifies the VRF to display. The default is default vrf.

Examples

Displaying the multicast static route and corresponding summarized route information for all vrfs:

```
switch# show ipv6 multicast-static-route all-vrfs

VRF : red

Group Address           : ff0e::c
Source Address          : 2001::2
Route type               : Static
Incoming interface      : vlan200
Outgoing Interface List :
Interface               State
-----
vlan10                  forwarding

VRF : blue

Group Address           : ff0e::c
Source Address          : Any
Route type               : Static-Summarized
Incoming interface      : vlan200
Outgoing Interface List :
Interface               State
-----
vlan10                  forwarding
```

Displaying the multicast static route information for a specific group:


```
switch# show ipv6 multicast-static-route ff0e::c all-vrfs
```

```
VRF : red
```

```
Group Address      : ff0e::c
Source Address     : 2001::2
Route type         : Static
Incoming interface : vlan200
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding
```

```
VRF : blue
```

```
Group Address      : ff0e::c
Source Address     : Any
Route type         : Static-Summarized
Incoming interface : vlan200
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding
```

Displaying the multicast static route information for a specific group and source:

```
switch# show ipv6 multicast-static-route ff0e::c 2001::2 all-vrfs
```

```
VRF : red
```

```
Group Address      : ff0e::c
Source Address     : 2001::2
Route type         : Static
Incoming interface : vlan100
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding
```

```
VRF : blue
```

```
Group Address      : ff0e::c
Source Address     : 200::2
Route type         : Static
Incoming interface : vlan200
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding
```

Displaying the multicast static route information for a specific group and any source:

```
switch# show ipv6 multicast-static-route ff0e::c any all-vrfs
```

```
VRF : red
```

```
Group Address      : ff0e::c
Source Address     : Any
Route type         : Static-summarized
```

```

Incoming interface      : 1/1/3
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding

VRF : blue

Group Address          : ff0e::c
Source Address         : Any
Route type             : Static-summarized
Incoming interface     : vlan200
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding

```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 multicast-static-route (group)

`show ipv6 multicst-static-route <GROUP-ADDRESS> {<SOURCE-ADDRESS | ANY>} [all vrfs | vrf <VRF-NAME>]`

Description

Displays the multicast static route and corresponding summarized route information for the given group address in the given VRF briefly. If VRF is not specified, the default VRF is displayed.

Parameter	Description
<GROUP-ADDRESS>	Specifies the group address.
<SOURCE-ADDRESS>	Specifies the source address.
<ANY>	Selects any source address.
[all vrfs]	Selects all VRFs to display.
[vrf <VRF-NAME>]	Specifies the VRF to display. The default is default vrf.

Examples

Displaying the multicast static route information for a specific group:

```
switch# show ipv6 multicast-static-route ff0e::c 2002::2 vrf red
```

```
VRF : red
```

```
Group Address          : ff0e::c
Source Address         : 2002::2
Route type             : Static
Incoming interface     : 1/1/2
Outgoing Interface List :
Interface      State
-----
vlan10        forwarding
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 multicast-static-route detail

```
show ipv6 multicast-static-route <GROUP-ADDRESS> {<SOURCE-ADDRESS> | ANY}> detail [all  
vrfs | vrf <VRF-NAME>]
```

Description

Displays the multicast static route and corresponding summarized route information for the given group address in the given VRF detail. If VRF is not specified, the default VRF is displayed.

Parameter	Description
<GROUP-ADDRESS>	Specifies the group address.
<SOURCE-ADDRESS>	Specifies the source address.
<ANY>	Selects any source address.
[all vrfs]	Selects all VRFs to display.
[vrf <VRF-NAME>]	Specifies the VRF to display. The default is default vrf.

Examples

Displaying the multicast static route information for a specific group:

```
switch# show ipv6 multicast-static-route ff0e::c 2002::2 detail vrf red
VRF : red

Group Address          : ff0e::c
Source Address         : 2002:2
Route type             : Static
Incoming interface     : 1/1/2
Outgoing Interface List :
Interface      State      Vsteps
-----
vni1000        forwarding  2.2.2.2, 3.3.3.3
```

Displaying the multicast static route information for any group on vrf red:

```
switch# show ipv6 multicast-static-route ff0e::c any detail vrf red
VRF : red

Group Address          : ff0e::c
Source Address         : Any
Route type             : Static
Incoming interface     : 1/1/2
Outgoing Interface List :
Interface      State      Vsteps
-----
vni1000        forwarding  2.2.2.2, 3.3.3.3
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config

show running-config

Description

Displays the running configuration.

Examples

Displaying the running configuration:

```
switch# show running-config
!
```

```

-----
-----
ip multicast-static-route vlan10 10.10.1.2 239.255.255.250 vlan20
ip multicast-static-route vlan10 10.10.1.2 239.255.255.250 1/1/2
ip multicast-static-route vlan21 any 239.255.255.250 1/1/2
ip multicast-static-route vlan30 10.10.1.2 239.255.255.250 1/1/16 vrf red
ip multicast-static-route 1/1/1 10.10.1.2 239.255.255.250 1/1/2
ipv6 multicast-static-route vlan10 2001::1 ff02::c vlan20
ipv6 multicast-static-route vlan50 any ff0e::c vlan70 vrf red
ipv6 multicast-static-route vlan50 any ff0e::c vlan80 vrf red
ipv6 multicast-static-route vlan10 2001::1 ff02::c vlan20
ipv6 multicast-static-route vlan10 2001::1 ff02::c 1/1/1

```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear mvrp statistics

clear mvrp statistics [*<PORT-NUM>* | *<PORT-LIST>* | LAG *<LAG-NUM>*]

Description

Resets the MVRP statistic counters globally or for the specified ports or LAG.

Parameter	Description
<i><PORT-NUM></i>	Specifies a port number.
<i><PORT-LIST></i>	Specifies a list of ports.
LAG <i><LAG-NUM></i>	Specifies a Link Aggregation number. Range: 1 to 128.

Examples

```
switch# clear mvrp statistics 1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

mvrp

mvrp
no mvrp

Description

Enables the MVRP feature globally or on a specific interface. By default, MVRP is disabled. The **no** form of this command disables MVRP.



MVRP and VLAN translation cannot be enabled on the same interface.

Examples

Enabling MVRP globally:

```
switch(config)# mvrp
```

Enabling MVRP on an interface:

```
switch(config)# interface 1/1/1  
switch(config-if)# mvrp
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config config-if	Administrators or local user group members with execution rights for this command.

mvrp registration

```
mvrp registration {normal | fixed | forbidden [<VLAN-LIST>]}  
no mvrp registration forbidden {<VLAN-LIST>}
```

Description

Configures the MVRP registrar state which determines how an MVRP participant responds to MRP messages. The default registration mode is normal.

The **no** command removes the specified VLANs from the forbidden list.

Parameter	Description
normal	Enables dynamic registration and deregistration of VLANs on the interface, and propagates VLAN information to other switches on the network. Default.

Parameter	Description
fixed	Disables dynamic deregistration of VLANs and drops received MVRP frames. The interface does not deregister dynamic VLANs or register new dynamic VLANs.
forbidden	Disables dynamic registration of VLANs and drops received MVRP frames. The MVRP participant does not register new dynamic VLANs or re-register a deregistered dynamic VLAN.
<VLAN-LIST>	Disables dynamic registration of VLANs and drops received MVRP frames for specific VLANs only. Normal behavior applies to all other VLANs. Specify the number of a single VLAN, or a series of numbers for a range of VLANs, separated by commas (1, 2, 3, 4), dashes (1-4), or both (1-4,6).

Examples

```
switch(config)# switch(config-if)# mvrp registration forbidden 10
```

```
switch(config-if)# mvrp registration fixed
```

```
switch(config-if)# mvrp registration forbidden 1,2,10-20
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

mvrp timer

```
mvrp timer {join | leave | leaveall | periodic} <TIME>
no mvrp timer {join | leave | leaveall | periodic}
```

Description

Sets an MVRP timer.

The **no** form of this command sets the specified timer to its default value.

Parameter	Description
<code>join <TIME></code>	Sets the join timer. You can use the timer to space MVRP join messages. To ensure that join messages are transmitted to other participants, an MRP participant waits for the specified period of the join timer before sending a join message. The Join timer must be less than half of the Leave Timer. Range: 20 to 100 in centiseconds. Default: 20.
<code>leave <TIME></code>	Sets the leave timer for the port, specifying the time that the registrar state machine waits in the LV state before transiting to the MT state. The leave timer must be at least twice the join timer and must be less than the leave all timer. Range: 40 - 1000000 centiseconds. Default: 300 centiseconds.
<code>leaveall <TIME></code>	Sets the leave all timer for the port, specifying the frequency with which the leave all state machine generates leave all PDUs. Range: 500 to 1000000 centiseconds. Default: 1000.
<code>periodic <TIME></code>	Sets the periodic timer for the port, specifying the frequency with which the periodic transmission state machine generates periodic events. The periodic timer is set to 1 second when it is started. Range: 100 to 1000000 centiseconds. Default: 100.

Examples

```
switch(config-if)# mvrp timer join 22
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-if</code>	Administrators or local user group members with execution rights for this command.

show mvrp config

```
show mvrp config [<PORT-NUM> | <PORT-LIST> | LAG <LAG-NUM>] [vsx-peer]
```

Description

Displays the MVRP configuration for all L2 ports or optionally for the ports specified.

Parameter	Description
<PORT-NUM>	Specifies displaying information for a particular port number.
<PORT-LIST>	Specifies displaying information for a list of ports.
LAG <LAG-NUM>	Specifies displaying information by LAG. Range: 1 to 128.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show mvrp config
Configuration and Status - MVRP
Global MVRP status : Disabled
Port      Status      Registration Join   Leave  LeaveAll Periodic
-----  -
Type
-----
1/1/1    Disabled    Normal      20    300    1000    100
1/1/2    Disabled    Normal      20    300    1000    100
1/1/3    Disabled    Normal      20    300    1000    100
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mvrp state

```
show mvrp state [<VLAN-ID> | <VLAN-ID> <PORT-NUM>] [vsx-peer]
```

Description

Displays the MVRP Registrar and Applicant state machine information for all ports on which MVRP is enabled, or for specific ports.

Parameter	Description
<VLAN-ID>	Specifies the number of a VLAN. Range: 1 - 4040.
<PORT-NUM>	Specifies a physical port on the switch. Format: member/slot/port .
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show mvrp state 1
Configuration and Status - MVRP state for VLAN 1
Port   VLAN Registrar Applicant
      State      State
----
1/1/1  1      MT      QA
```

```
switch# show mvrp state 10 1/1/1
Configuration and Status - MVRP state for VLAN 10
Port   VLAN Registrar Applicant Forbid
      State      State      Mode
----
1/1/1  10      MT      LO      Yes
switch#
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mvrp statistics

show mvrp statistics [<PORT-LIST>] [vsx-peer]

Description

Displays MVRP statistics for all ports or on the ports specified in the list.

Parameter	Description
<PORT-LIST>	Specifies a list of ports. When specifying a list of ports, the ports for which there are no statistics will be listed in the output.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show mvrp statistics
Status and Counters - MVRP
MVRP statistics for port : 1/1/1
-----
Failed registration      : 0
Last PDU origin         : 48:0f:cf:af:b1:76
Total PDU Transmitted   : 13127
Total PDU Received      : 327
Frames Discarded        : 0
Message type            Transmitted      Received
-----
New                      0              0
Empty                    50029394         1264
In                        0              4
Join Empty               1425             48
Join In                   563             555
Leave                      0              0
Leaveall                  12218            25
```

```
switch# show mvrp statistics 1/1/1

Status and Counters - MVRP
MVRP statistics for port : 1/1/1
-----
Failed registration      : 0
Last PDU origin         : 48:0f:cf:af:b1:76
Total PDU Transmitted   : 14874
Total PDU Received      : 327
Frames Discarded        : 0
Message type            Transmitted      Received
-----
New                      0              0
Empty                    57181612         1264
In                        0              4
Join Empty               1425             48
Join In                   563             555
Leave                      0              0
Leaveall                  13965            25
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear nd-snooping statistics

clear nd-snooping statistics

Description

Clears all ND snooping statistics.

Examples

Clear all ND snooping statistics:

```
switch# clear nd-snooping statistics
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

nd-snooping

nd-snooping {enable|disable}
no nd-snooping {enable|disable}

Description

Enables or disables ND snooping. ND snooping is disabled by default. ND snooping is not supported on the management interface.

Examples

Enabling ND snooping:

```
switch(config)# nd-snooping enable
```

Disabling ND snooping:

```
switch(config)# nd-snooping disable
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

nd-snooping (in config-vlan context)

nd-snooping
no nd-snooping

Description

Enables ND snooping in the **config-vlan** context. ND snooping is disabled by default for all VLANs. The no form of the command disables ND snooping on the specified VLAN.

Examples

Enabling ND snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Disabling ND snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no nd-snooping
switch(config-vlan-100)# exit
switch(config)#
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-vlan	Administrators or local user group members with execution rights for this command.

nd-snooping mac-check

nd-snooping mac-check
no nd-snooping mac-check

Description

This command enables verification of the hardware address field in ND snooping packets. When enabled, the ICMPv6 target link layer address field and the source MAC address must be the same for packets received on untrusted ports or else the packets are dropped. This ND snooping MAC verification is enabled by default.

The no form of the command disables ND snooping MAC verification.

Examples

Enabling ND snooping MAC verification:

```
switch(config)# nd-snooping mac-check
```

Disabling ND snooping MAC verification:

```
switch(config)# no nd-snooping mac-check
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

nd-snooping ra-guard

nd-snooping ra-guard [log]
no nd-snooping ra-guard

Description

This command enables Routing Advertisement (RA) guard on the selected VLAN. When enabled, ingress Routing Advertisement (RA) and Routing Redirect (RR) packets on the selected VLAN are blocked on untrusted ports. The packets are forwarded when received on trusted ports.

The no form of the command disables RA guard on the VLAN.



ND snooping must be enabled in both the global context and the config-vlan context before this command can be used.

Parameter	Description
[log]	Logs messages along with drop functionality.

Examples

Enabling ND snooping RA guard on VLAN 100:

```
switch(config)# nd-snooping enable
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping ra-guard
switch(config-vlan-100)# exit
switch(config)#
```

Enabling ND snooping RA guard on VLAN 100 with event logging on dropped packets:

```
switch(config)# nd-snooping enable
switch(config)# vlan 100
switch(config-vlan-100)# nd-snooping ra-guard log
switch(config-vlan-100)# exit
switch(config)#
```

Disabling ND snooping RA guard on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no nd-snooping ra-guard
switch(config-vlan-100)# exit
switch(config)#
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-vlan-<VLAN-ID>	Administrators or local user group members with execution rights for this command.

nd-snooping trust

```
nd-snooping trust
no nd-snooping trust
```

Description

Enables ND snooping trust on the selected interface (port) allowing RA and RR packets to be received. RA and RR packets received on untrusted ports are discarded, all ports are untrusted by default. The no form of the command disables ND snooping trust on the selected port.

Examples

Enabling ND snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# nd-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling ND snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no nd-snooping trust
switch(config-if)# exit
switch(config)#
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

show nd-snooping

```
show nd-snooping [vlan <VLAN-ID>] [vsx-peer]
```

Description

Shows either all ND snooping configuration or the configuration for the specified VLAN.

Parameter	Description
vlan <VLAN-ID>	Specifies the VLAN for which the ND configuration is to be shown. Range: 1 to 4094.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

(Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series.) Showing all ND snooping configuration:

```
switch(config)# show nd-snooping

ND Snooping Information
=====

ND Snooping           : Enabled
ND Snooping Enabled VLANs : 10
RA Guard Enabled VLANs  : 10
MAC Address Check      : Disabled

PORT    TRUST
-----  -
1/1/1    Yes
1/1/2    Yes
1/1/3    No
1/1/4    No
1/1/5    No
```

(Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series.) Showing ND snooping configuration for VLAN 2:

```
switch(config)# show nd-snooping vlan 2

ND Snooping Information
=====

ND Snooping           : Enabled
MAC Address Check     : Disabled
RA Guard              : Disabled

PORT    TRUST
-----  -
1/1/1    Yes
1/1/2    Yes
1/1/3    No
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show nd-snooping statistics

show nd-snooping statistics [vsx-peer]

Description

Shows the global ND snooping statistics.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

(Applies to the HPE Aruba Networking 8325, 9300/9300S, 10000 Switch series.) Showing global ND snooping statistics:

```
switch(config)# show nd-snooping statistics
```

PACKET-TYPE	ACTION	REASON	COUNT
RA	forward	RA packets received on trusted port	20
RA	drop	RA packets received on untrusted port	45
RR	forward	RR packets received on trusted port	20
RR	drop	RR packets received on untrusted port	45



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

nae cli-authorization

nae cli-authorization
no nae cli-authorization

Description

Configures the NAE agent action CLI commands to require authorization. By default, the NAE agent action CLI commands are subject to regular command authorization, including when TACACS+ is configured for authorization. Unless the configured authorization method allows the CLI commands sent by the NAE agent as user admin, the NAE agent action CLI commands will result in command failures.

The **no** form of the command disables the authorization required for NAE agent action CLI commands.

Examples

Enabling authorization requirement for NAE agent action CLI commands:

```
switch(config)# nae cli-authorization
```

Disabling authorization requirement for NAE agent action CLI commands:

```
switch(config)# no nae cli-authorization
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show nae-agent

```
show nae-agent [<AGENT-NAME>] [vsx-peer]
```

Description

Shows the details of the NAE Agent. If the agent name is specified, then shows the information details of the specified agent.

Parameter	Description
<code><AGENT-NAME></code>	Specifies the name of the agent. Length: 3 to 80 alphanumeric characters, including underscore (_).
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

The output of this command shows the following information about the HPE Aruba Networking Network Analytics Engine agents that are configured and enabled on the switch:

Parameter	Description
Agent Name	The name of the agent. Length: 3 through 80 characters.
Script Name	The name of the script. Length: 3 through 80 characters. Example: memory_monitor
Version	The version number of the script.
Origin	The origin of the script: ▪ system: Indicates that the script is provided as part of the system software. ▪ user: Indicates that a user loaded the script. ▪ generated: Indicates that the agent is configured using the CLI.
Disabled	Indicates whether the agent is disabled or enabled on the switch: ▪ true: Indicates that the agent is disabled. ▪ false: Indicates that the agent is enabled on the switch.
Status	The current state of the agent. Status values are the following: ▪ CRITICAL :The agent has encountered a critical error during execution. For information about the error, see the Analytics Dashboard of the Web UI. ▪ MAJOR: The agent has encountered a major error during execution. For information about the error, see the Analytics Dashboard of the Web UI. ▪ MINOR: The agent has encountered a minor error during execution. For information about the error, see the Analytics Dashboard of the Web UI. ▪ NORMAL: Indicates that the agent is actively monitoring network conditions and handling events.

Parameter	Description
Time series count	Number of time series associated with agent.
Alerts count	Number of alerts generated by the agent.
Rules	Number of Prometheus rules associated with the agent.
Error	Current error state of the agent.
Recent alerts	Lists the recent alerts.

Example

Showing the details of all the NAE agents existing in the switch:

```
switch# show nae-agent
-----
Agent Name                               Script Name                               Version
Origin   Disabled  Status    Time Series Count  Alerts Count  Rules  Error
-----
com.arubanetworks.monitor.agent         com.arubanetworks.monitor               1.0
user      true      UNKNOWN   0                  0             0      NONE
interface_monitor.agent                 interface_tx_rx_stats_monitor            2.3
user      true      UNKNOWN   168                10            36      NONE
com.arubanetworks.wildcard.vlan.agent    com.arubanetworks.wildcard.vlan          1.0
user      false     UNKNOWN   0                  0             0      ERROR
system_resource_monitor.default          system_resource_monitor                  1.3
system    false     NORMAL    6                  23            10      NONE
event_monitor                           event_monitor                           NA
generated NA          NA        0                  0             0      Script
activation is pending
cpu_monitor                             cpu_monitor                             NA
generated NA          NA        0                  0             0      Script
generation is in progress
mem_monitor                             mem_monitor                             NA
generated NA          NA        0                  0             0      Script
validation is in progress
interface_monitor                       interface_monitor                       NA
generated NA          NA        0                  0             0      Agent
creation is in progress
port_monitor                            port_monitor                            NA
generated NA          NA        0                  0             0      Agent
updatation is in progress
```

Showing the details of the NAE agent named **memory_monitor**:

```
switch# show nae-agent memory_monitor
Script Name      : memory_monitor
Version          : 1.0
Origin           : generated
Disabled         : false
Status           : NORMAL
Time Series Count : 0
Alerts Count     : 0
Rules            : 0
Error            : None
```



```
Alert Description : Memory - Normal
Recent alerts      :
<1> 2021-05-29 01:34:11 An action has been triggered by NAE agent memory_monitor
<2> 2021-05-28 06:11:00 An action has been triggered by NAE agent memory_monitor
<3> 2021-05-27 03:19:50 An action has been triggered by NAE agent memory_monitor
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.13.1000	Command output updated to display Alert Description for the agent name.
10.09	Added <code><AGENT-NAME></code>
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show nae-agent alerts

`show nae-agent [<AGENT-NAME>] alerts`

Shows the alerts raised by all the NAE agents. If the agent name is specified, then shows the alerts raised by the specified agent.

Parameter	Description
<code><AGENT-NAME></code>	Specifies the name of the NAE-Lite agent.

Example

Showing the alerts raised by all the NAE agents:

```
switch# show nae-agent alerts
2021-06-13 07:53:56 An action has been triggered by NAE agent memory_monitor
2021-06-07 00:30:10 An action has been triggered by NAE agent system_resource_
monitor.default
2021-06-07 00:24:13 An action has been triggered by NAE agent system_resource_
monitor.default
2021-06-06 21:48:27 An action has been triggered by NAE agent memory_monitor
2021-06-06 18:44:41 An action has been triggered by NAE agent system_resource_
```

```
monitor.default
2021-06-06 18:31:53 An action has been triggered by NAE agent system_resource_
monitor.default
2021-06-06 20:19:03 An action has been triggered by NAE agent system_resource_
monitor.default
2021-06-06 20:15:05 An action has been triggered by NAE agent system_resource_
monitor.default
2021-06-03 07:45:36 An action has been triggered by NAE agent memory_monitor
```

Showing the alerts raised by the NAE agent named **memory_monitor**:

```
switch# show nae-agent memory_monitor alerts
2021-06-13 07:54:47 An action has been triggered by NAE agent memory_monitor
2021-06-13 07:53:56 An action has been triggered by NAE agent memory_monitor
2021-06-06 21:48:27 An action has been triggered by NAE agent memory_monitor
2021-06-03 07:45:36 An action has been triggered by NAE agent memory_monitor
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show nae-agent alerts details

```
show nae-agent [<AGENT-NAME>] alerts details [<INSTANCE-ID>]
```

Description

Shows the detailed information of a specific NAE agent alert raised by all the NAE agents.



Only CLI, alert, and system log specific action details are displayed as the output. For other action details, refer to the Web UI.

Parameter	Description
<AGENT-NAME>	Specifies the name of the NAE-Lite agent. Length: 3 to 80 alphanumeric characters, including underscore (_).

Parameter	Description
<INSTANCE-ID>	Specifies the instance of the alert. Number 1 represents the latest alert whereas N represents the Nth recent alert. By default, it displays the latest alert (<i>INSTANCE-ID=1</i>).

Example

Showing the details of the recent alert of the NAE-Lite agent named **memory_monitor**:

```
switch# show nae-agent memory_monitor alerts details 1
2Alert Message: 2021-06-13 07:54:47 An action has been triggered by NAE agent
memory_monitor
Action(s) performed: Alert, CLI, Syslog

Action Details:
=====
Action Alert: Alert level changed to MAJOR
Action Syslog: Potential mis-configuration detected
Action CLI:
6405# top cpu
top - 07:54:27 up 25 min,  1 user,  load average: 10.45, 10.38, 8.48
Tasks: 295 total,  1 running, 294 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.2 us,  2.2 sy,   0.0 ni, 95.7 id,   0.0 wa,   0.0 hi,   0.0 si,   0.0 st
MiB Mem :  7555.6 total,  1982.1 free,  2022.6 used,  3550.9 buff/cache
MiB Swap:    0.0 total,    0.0 free,    0.0 used.  5307.9 avail Mem

   PID USER      PR  NI   VIRT   RES   SHR S  %CPU  %MEM    TIME+  COMMAND
 27776 admin      20   0   3540   2128  1580 R   16.7   0.0   0:00.04
/usr/bin/top -b -n 2 -c -o %CPU -w 11+
   1 root        20   0  14272   9468  5260 S    0.0   0.1   0:03.23  /sbin/init
   2 root        20   0     0     0     0 S    0.0   0.0   0:00.00  [kthreadd]
   3 root         0 -20     0     0     0 I    0.0   0.0   0:00.00  [rcu_gp]

Only the action Alert, action Syslog, and action CLI details are displayed in this
command.
Please refer to the Web UI for other action details.
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show nae-script

show nae-script [vsx-peer]

Description

Shows information about the HPE Aruba Networking Network Analytics Engine scripts that are available on the switch.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

This command shows the following information about the HPE Aruba Networking Network Analytics Engine scripts that are available on the switch:

Script Name

The name of the script. Length: 3 through 80 characters.

Example: **system_resource_monitor_mm1.default**

Version

The version number of the script.

Origin

The origin of the script:

system

Indicates that the script is provided as part of the system software.

user

Indicates that a user loaded the script.

Status

The current state of the script. Status values are the following:

CREATED

The script has been uploaded to the switch, but script validation has not begun.

ERROR

The script validation process detected an error that would result in execution errors if an agent runs the script. Resolve the error by modifying the script. For information about the error, see the **Analytics Dashboard** of the Web UI.

VALIDATING

The script syntax and components (manifest, parameters, monitor, condition, and action) are in the process of being validated.

VALIDATED

The script syntax and components (manifest, parameters, monitor, condition, and action) have been validated and no errors have been found.

Example

```
switch# show nae-script
```

```
-----  
Script Name                               Version  Origin    Status
```

```

-----
fan_monitor                1.0      system  VALIDATED
interface_link_flap_monitor 1.0      system  VALIDATED
interface_link_state_monitor 1.0      system  VALIDATED
interface_tx_rx_stats_monitor 1.0      system  VALIDATED
lag_imbalance_monitor       1.0      system  VALIDATED
lag_status_monitor          1.0      system  VALIDATED
power_supply_monitor         1.0      system  VALIDATED
stp_bpdu_tcn_rate_monitor    1.0      system  VALIDATED
system_resource_monitor_mm1.default 1.0      system  VALIDATED
system_resource_monitor_mm2.default 1.0      system  VALIDATED
temp_sensor_monitor          1.0      system  VALIDATED
-----
Script Name                Version  Origin  Status
-----
fan_monitor                1.0      system  VALIDATED
interface_link_flap_monitor 1.0      system  VALIDATED
interface_link_state_monitor 1.0      system  VALIDATED
interface_tx_rx_stats_monitor 1.0      system  VALIDATED
lag_imbalance_monitor       1.0      system  VALIDATED
lag_status_monitor          1.0      system  VALIDATED
power_supply_monitor         1.0      system  VALIDATED
stp_bpdu_tcn_rate_monitor    1.0      system  VALIDATED
system_resource_monitor_mm1.default 1.0      system  VALIDATED
system_resource_monitor_mm2.default 1.0      system  VALIDATED
temp_sensor_monitor          1.0      system  VALIDATED

```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

uerieshow running-config (nae-lite)

`show running-config`

Description

Shows the NAE-Lite running configuration.

Example

Showing the NAE-Lite running configuration:

```

switch# show running-config
Current configuration:
!
!Version Halon 0.1.0 (Build: ridley-Halon-0.1.0-master-20161110190644-dev)
!Schema version 0.1.8
hostname switch
...
nae-agent memory_monitor
  desc Memory resource monitor
  monitor memory system memory line-module 1/3
  set-condition monitor memory gt 80
    status major
    syslog "High memory usage detected"
  cli show system
  clear-condition monitor memory lt 40
    status normal
    syslog "Memory usage is recovered to normal limit"
exit
nae-agent crash_watch
  desc Watch the crash event
  tags crash, resource
  watch crash_event event-log 1201
  set-condition watch event-log crash_event
    status major
    cli show core-dump all
exit
nae-agent crash_watch activate
nae-agent memory_monitor activate
...

```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

actions

```
status {normal | minor | major | critical}
no status {normal | minor | major | critical}

syslog <MESSAGE> [facility {kern | user | mail | daemon | auth | syslog |
    lpr | uucp | authpriv | cron | ftp}]
    [severity {debug | info | notice | warning | err | crit | alert | emer}]
no syslog <MESSAGE> [facility {kern | user | mail | daemon | auth | syslog |
    lpr | uucp | authpriv | cron | ftp}]
    [severity {debug | info | notice | warning | err | crit | alert | emer}]

cli <COMMAND> {show system | redirect local-file} {show version | redirect tftp}
no cli <COMMAND>

schedule <SCHEDULE>
no schedule <SCHEDULE>

trap <TRAP>
no trap <TRAP>
```

Description

Configures different NAE-Lite agent actions to be performed when the set condition or the clear condition is met. The following NAE actions can be configured for the set and clear condition:

status—Set the alert level for the NAE-Lite Agent.

syslog—Create a syslog message and send it to the configured remote syslog servers.

cli—Execute a CLI command. Multiple CLI commands can be specified by using **\n** as the delimiter.

schedule—Execute a configured job CLI commands at the specific time.

trap—Create a snmp trap message and send it to the configured snmp servers.

redirect local-file —Store output in the local file.

redirect {tftp | sftp | scp} —Copy the output to a remote destination.

redirect tftp://<IP>/file%Date%.txt—Append the date, time, and hostname of the file.

The **no** form of this command removes the actions associated with the NAE-Lite agent condition.

Parameter	Description
normal	Sets the NAE-Lite agent status to normal (default).
minor	Sets the NAE-Lite agent status to minor .
major	Sets the NAE-Lite agent status to major .

Parameter	Description
<code>critical</code>	Sets the NAE-Lite agent status to critical .
<code><MESSAGE></code>	Specifies the syslog message to be sent when the set condition or the clear condition is met. Length: 3 to 255 characters.
<code>facility {kern user mail daemon auth syslog lpr uucp authpriv cron ftp}</code>	Specifies the syslog facility code to denote the type of program that is logging the message. The default facility code is daemon. Optional. The valid facility code values are: ▪ kern: Sets the syslog message source as kernel. ▪ user: Sets the syslog message source as user space programs. ▪ mail: Sets the syslog message source as mail system. ▪ daemon: Sets the syslog message source as system daemon (default). ▪ auth: Sets the syslog message source as authentication subsystem. ▪ syslog: Sets the syslog message source as syslog daemon. ▪ lpr: Sets the syslog message source as line printer subsystem. ▪ uucp: Sets the syslog message source as unix-to-unix copy subsystem. ▪ authpriv: Sets the syslog message source as security subsystem. ▪ cron: Sets the syslog message source as cron scheduler subsystem. ▪ ftp: Sets the syslog message source as FTP daemon.
<code>[severity {debug info notice warning err crit alert emer}]</code>	Specifies the severity level for the syslog message. The severity level values are: ▪ debug: Sets the syslog severity level as debug. ▪ info: Sets the syslog severity as information (default). ▪ notice: Sets the syslog severity as notice. ▪ warning: Sets the syslog severity as warning. ▪ err: Sets the syslog severity as error. ▪ crit: Sets the syslog severity as critical. ▪ alert: Sets the syslog severity as alert. ▪ emer: Sets the syslog severity as emergency.
<code><COMMAND></code>	Specifies the CLI command to be executed when the set condition or the clear condition is met.
<code>{show system redirect local-file}</code>	Specifies where to relocate local-file.
<code>{show version redirect tftp}</code>	Specifies where to relocate tftp.

Usage

Take note of the following requirements and recommendations:

- Syslog messages should be a minimum of 3 to a maximum of 255 characters. Syslog facility code can be specified to denote the type of program that is logging the message. Remote syslog server could use this facility to separate the syslogs into separate log buffers. Default facility code is `daemon`. Syslog severity can be used to denote the severity of the syslog message. Default severity is `info`.
- SNMP trap messages should be a minimum of 3 and a maximum of 255 characters.
- Add the job configuration separately in the configuration node and execute the corresponding job name in the action schedule CLI.
- It is not recommended to use NAE-lite action schedule CLI commands in the NAE-lite action CLI.
- It is not recommended to add the job configuration CLI and schedule configuration CLI together in the action schedule CLI.
- Using action schedule CLI, the NAE-lite agent should load the recommended configuration from a specified location(remote destination) to the switch. The action schedule executes the pre-configured job CLI, which executes a copy of the default config to running-config. Only TFTP is allowed for the job CLI execution.

NAE-Lite Action CLI Execution for SFTP/SCP

- SFTP/SCP transfer method is used to securely copy files from switch to remote server and requires a password.
- NAE-Lite agent CLI execution is not a user-interactive command and password prompt is not allowed to copy the file. Use SSH key-based authentication to copy the file from switch to a remote destination.
- Before executing NAE-Lite action CLI for SFTP/SCP transfer methods, specify the remote-server user information using CLI 'remote-server user USERNAME password (plaintext|ciphertext) PASSWORD [host WORD]'.



It is recommended to use secure-prompt and Ciphertext options as these are more secure. The plaintext option does not hide the password in the CLI.

The following steps are internal workflow for NAE-lite action CLI execution for SFTP/SCP:

1. The `remote-server user USERNAME password (plaintext|ciphertext) PASSWORD [host WORD]` CLI is used to store the remote username, password and hostname(optional) in the OVSDb and generate an SSH Key on the Switch. The generated `id\_rsa` and `id\_rsa.pub` SSH keys are stored in the `/fs/nos/` file system.
2. During the execution of action CLI, read the remote username and password from the OVSDb using sshpass establish the connection between switch and remote server.
3. Copy the public key to the remote server.
4. Copy the action CLI output file from switch to a remote destination.

Please note the following:

1. The usage of the public key with the SFTP/SCP client implies that there will only be one key.
2. This will not work with users authenticating with AAA, enhanced secure mode, and RADIUS authentication.
3. In HA scenarios, the public key will be synced between Active and Standby Modules.
4. The remote username and password should not be deleted from the OVSDb during the execution of NAE-lite action CLI.

5. The SSH public key, should not be deleted from the file system during the execution of NAE-lite Action CLI.
6. During the execution of NAE-lite action CLI, the output file will be copied to the remote destination only for the matched remote user information specified in the OVSDb.
7. Multiple remote servers are not allowed. If the user updates the new remote server configuration, it will overwrite the existing remote server from the OVSDb.

Examples

Setting the status level for the NAE-Lite agent condition:

```
switch(config-nae-agent-condition) # status major
```

Creating the syslog message for the NAE-Lite agent condition:

```
switch(config-nae-agent-condition) # syslog "IPSLA server1 is down" severity err
```

Executing the CLI command for the NAE-Lite agent condition:

```
switch(config-nae-agent-condition) # cli show version\nshow image
```

Removing the different actions associated with the NAE-Lite agent condition:

```
switch(config-nae-agent-condition) # no status minor
```

```
switch(config-nae-agent-condition) # no syslog "Processing system event"
```

```
switch(config-nae-agent-condition) # no cli show logging
```

Executing the schedule CLI command:

```
switch(config-nae-agent-condition) # schedule  
SCHEDULE Set the job schedule CLI command. The CLI commands can be specified by  
using ``\n`` as the separator.
```

Example of a scheduled CLI Command:

```
switch(config-nae-agent-condition) # schedule s1\n10 job j1\ntrigger every minutes  
30 start 17:20 2023-11-21
```

Example of a trap message:

```
switch(config-nae-agent-condition) # trap High system CPU utilization
```

Removing the scheduled CLI command:

```
switch(config-nae-agent) # no schedule
```

Removing snmp trap message:

```
switch(config-nae-agent) # no trap
```

User configured NAE-Lite agent CLI with date format:

```
nae-agent lite event_crash
  watch crash event-log 1201
  set-condition watch event-log crash
    status minor
    syslog "crash triggered run to start"
    cli show version | redirect tftp://10.0.0.2/file%Date%.txt
!
nae-agent lite event_crash activate
```

Running-config for above NAE-agent:

```
nae-agent lite event_crash
  watch crash event-log 1201
  set-condition watch event-log crash
    status minor
    syslog "crash triggered run to start"
    cli show version | redirect tftp://10.0.0.2/file_2024-05-16_101230_
6300.txt
!
nae-agent lite event_crash activate
```

NAE-Lite agent load recommended configuration using action schedule:

```
job j1
  10 cli copy tftp://10.0.0.2/run_cfg.txt running-config

nae-agent lite switch_boot_up
  watch switch_up event-log 4311
  set-condition watch event-log switch_up
    status major
    syslog "switch is up and load recommended configuration from a specified
location."
    schedule config\nschedule s1\n10 job j1\ntrigger every minutes 30 start
12:30 2024-05-16
!
nae-agent lite switch_boot_up activate
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.15	Added support for TFTP/SFTP/SCP .
10.14	Schedule and Trap actions introduced.
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent-condition	Administrators or local user group members with execution rights for this command.

desc

```
desc <DESCRIPTION>
no desc <DESCRIPTION>
```

Description

Adds the description for the NAE-Lite agent.

The **no** form of this command removes the description from the NAE-Lite agent.

Parameter	Description
<DESCRIPTION>	Specifies the description for the NAE-Lite agent. Range: 3 to 255 characters

Example

Adding the description for the NAE-Lite agent:

```
switch(config-nae-agent)# desc Monitor system memory
```

Removing the description for the NAE-Lite agent:

```
switch(config-nae-agent)# no desc Monitor system memory
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent	Administrators or local user group members with execution rights for this command.

disable

disable
no disable

Description

Disables the NAE-lite agent. The NAE-Lite agents are enabled by default. The **no** form of this command enables the NAE-Lite agent.

Example

Disabling the NAE-Lite agent:

```
switch(config-nae-agent) # disable
```

Enabling the NAE-Lite agent:

```
switch(config-nae-agent) # no disable
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent	Administrators or local user group members with execution rights for this command.

monitor resource

```
monitor <MONITOR-NAME> resource <RESOURCE> [group-by {count | sum | min | max | average}
[over {seconds | minutes | hours | days} <DURATION>]]
no monitor <MONITOR-NAME> resource <RESOURCE> [group-by {count | sum | min | max |
average} [over {seconds | minutes | hours | days} <DURATION>]]
```

```
monitor <MONITOR-NAME> resource <RESOURCE> group-by rate over {seconds | minutes | hours
| days} <DURATION>
```

```
no monitor <MONITOR-NAME> resource <RESOURCE> group-by rate over {seconds | minutes |
hours | days} <DURATION>
```

Description

Configures the monitor for the NAE-Lite agent. The monitor defines what system resource the agent must monitor. Monitors are defined using the time series function and it supports the grouping of data. The **no** form of this command removes the monitor associated with the NAE-Lite agent. Before removing the monitor, you must remove the condition used in the monitor.

Parameter	Description
<code><MONITOR-NAME></code>	Specifies the name of the monitor. Length: 3 to 80 alphanumeric characters, including underscore (_).
<code><RESOURCE></code> The <code><RESOURCE></code> is defined as follows: - For 8100, 8320, 8325, 8325H, 8325P, 8360, and 9300/9300S Switch Series: <code>system {cpu memory}</code> <code>system storage {nos security coredump logs selftest}</code>	Specifies the system resources such as memory, CPU, and storage utilization for specific modules that need to be monitored. Values are: cpu: Configures the CPU monitoring. memory: Configures the memory monitoring. storage: Configures the storage utilization monitoring. nos: Monitors the network operating system storage utilization. security: Monitors the security storage utilization. coredump: Monitors the coredump storage utilization. logs: Monitors the log storage utilization. selftest: Monitors the self-test storage utilization.
<code>group-by {count sum min max average}</code>	Groups the monitored data based on the parameters specified. Values are: count: Groups by distinct counts of monitored data. sum: Groups by summing the monitored data. min: Groups by minimum value of the monitored data. max: Groups the data by maximum value of the monitored data.

Parameter	Description
	▪ average: Groups by average value of the monitored data.
<code>over {seconds minutes hours days} <DURATION></code>	Group over the specified time interval in the past instead of the current value. Values are: seconds: Sets the time interval in seconds. Range: 5 to 10000 minutes: Sets the time interval in minutes. Range: 1 to 10000. hours: Sets the time interval in hours. Range: 1 to 10000. days: Sets the time interval in days. Range: 1 to 365.
<code>rate over {seconds minutes hours days} <DURATION></code>	Groups by rate of change of the monitored data over the specified time interval.

Example

Configuring the monitor for the system CPU usage:

```
switch(config-nae-agent) # monitor sys_cpu resource system cpu
```

Configuring the monitor for calculating the average CPU usage over the 30 minutes duration (8100, 8320, 8325, 8325H, 8325P, 8360, and 9300/9300S Switch Series):

```
switch(config-nae-agent) # monitor avg_sys_cpu resource system cpu group-by
average over minutes 30
```

Removing the monitor named **sys_mem**:

```
switch(config-nae-agent) # no monitor sys_mem
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent	Administrators or local user group members with execution rights for this command.

nae-agent lite

```
nae-agent lite <AGENT-NAME>
no nae-agent lite [<AGENT-NAME>]
```

Description

Configures the NAE-Lite agent. After the command is executed, the command prompt enters into the **nae-agent** context. The specified name of the agent is also used as the name of the NAE script generated from the agent configurations. Therefore the agent name must be unique and must not match with any existing NAE scripts or NAE-Lite agent names.

The **no** form of the command removes the NAE-Lite agent configuration. The **no nae-agent lite** command removes all the configured NAE-Lite agents.

Parameter	Description
<AGENT-NAME>	Specifies the name of the NAE-Lite agent. Length: 3 to 80 alphanumeric characters, including underscore (_).

Example

Configuring NAE-Lite agent named **mem_monitor** and entering into the **nae-agent** context:

```
switch(config)# nae-agent lite mem_monitor
switch(config-nae-agent)#
```

Removing the NAE-Lite agent named **mem_monitor**:

```
switch(config-nae-agent)# no nae-agent lite mem_monitor
```

Removing all the NAE-Lite agent configurations:

```
switch(config)# no nae-agent lite
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

nae-agent lite activate

```
nae-agent lite <AGENT-NAME> activate  
no nae-agent lite <AGENT-NAME> activate
```

Description

Activates the NAE-Lite agent creation. Once activated, the NAE-Lite agent gets generated, validated, and begins monitoring.

Whenever modifying the NAE-Lite agent configuration, after all the modifications are done, you must trigger the agent update process by executing **no nae-agent lite <AGENT-NAME> activate** followed by **nae-agent lite <AGENT-NAME> activate**. The agent will not be created or updated until the **nae-agent lite <AGENT-NAME> activate** command is executed.

The **no** form of the command deactivates the NAE-Lite agent. Once the command is executed, the NAE-Lite agent and its corresponding script will be deleted.

Parameter	Description
<AGENT-NAME>	Specifies the name of the NAE-Lite agent. Length: 3 to 80 alphanumeric characters, including underscore (_).

Example

Activating the NAE-Lite agent named **crash_watch** :

```
switch(config)# nae-agent lite crash_watch activate
```

Deactivating the NAE-Lite agent named **mem_monitor** :

```
switch(config)# no nae-agent lite mem_monitor activate
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

2set-condition monitor

```
set-condition monitor <MONITOR-NAME> {{lt | le | eq | ne | gt | ge} <VALUE>[for {seconds
| minutes | hours | days} <DURATION>] | transition from <STRING-LIST> to <STRING-LIST>}
no set-condition monitor <MONITOR-NAME> {{lt | le | eq | ne | gt | ge} <VALUE> [for
{seconds | minutes | hours | days} <DURATION>] | transition from <STRING-LIST> to
<STRING-LIST>}
```

```
clear-condition monitor <MONITOR-NAME> {{lt | le | eq | ne | gt | ge} <VALUE> [for
{seconds | minutes | hours | days} <DURATION>] | transition from <STRING-LIST> to
<STRING-LIST>}
no clear-condition monitor <MONITOR-NAME> {{lt | le | eq | ne | gt | ge} <VALUE> [for
{seconds | minutes | hours | days} <DURATION>] | transition from <STRING-LIST> to
<STRING-LIST>}
```

Description

Defines the condition for the monitor resource events. Once the condition is met, one or more actions are executed based on the configuration.

The clear condition is an optional component of the condition and helps in identifying if an event, usually an issue in the system, is no longer occurring. Clear conditions also address the problem when data is fluctuating above and below the threshold, generating too many alerts. Initially, when an NAE-Lite agent is created, only the set-condition is active. Once the set-condition is met, the condition becomes inactive and the clear condition becomes active. The set-condition becomes active again once the clear condition is met.

The **no** form of this command removes the monitor condition associated with the NAE-Lite agent.

Parameter	Description
<MONITOR-NAME>	Specifies the monitor name used in the condition.
<VALUE>	Specifies the numeric value compared with the monitor value. The defined values are: - lt (less than) - le (less than or equal to) - eq (equal to) - ne (not equal to) - gt (greater than) - ge (greater than or equal to) - transition
<DURATION>	Specifies the time duration. The defined time duration are: - seconds (Range: 5-10000) - minutes (Range: 1-10000) - hours (Range: 1-10000) - day
<STRING-LIST>	Specifies the list of one or more strings representing the initial or final value of the monitor. The strings are comma-separated and each string must be contained within double-quotes.

Example

Configuring set conditions for the NAE-Lite agent:

```
switch(config-nae-agent) # set-condition monitor average_mem gt 70
```

Configuring the set and clear conditions for the NAE-Lite agent:

```
switch(config-nae-agent) # set-condition monitor cpu gt 70 for minutes 30
switch(config-nae-agent-condition) # clear-condition monitor cpu lt 30 for minutes
30
```

```
switch(config-nae-agent) # set-condition monitor line_md1_state transition from
"ready" to "down","error"
switch(config-nae-agent-condition) # clear-condition monitor line_md1_state
transition from "down","error" to "ready"
```

Removing the monitor conditions for the NAE-Lite agent:

```
switch(config-nae-agent) # no set-condition monitor line_md1_state transition from
"ready" to "down","error"
```

```
switch(config-nae-agent-condition) # no clear-condition monitor cpu lt 30 for
minutes 30
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent config-nae-agent- condition	Administrators or local user group members with execution rights for this command.

5set-condition watch

```
set-condition watch event-log <WATCH-NAME> [include {all | any} <REGEX-LIST>] [exclude
<REGEX-LIST>] [count <COUNT>]
no set-condition watch event-log <WATCH-NAME> [include {all | any} <REGEX-LIST>] [exclude
<REGEX-LIST>] [count <COUNT>]
```

```
clear-condition watch event-log <WATCH-NAME> [include {all | any} <REGEX-LIST>] [exclude <REGEX-LIST>] [count <COUNT>]
no clear-condition watch event-log <WATCH-NAME> [include {all | any} <REGEX-LIST>] [exclude <REGEX-LIST>] [count <COUNT>]
```

Description

Defines the condition for the watch resource events. Once the condition is met, one or more actions are executed based on the configuration.

The clear condition is an optional component of the condition and helps in identifying an event, usually an issue in the system, is no longer occurring. Clear conditions also address the problem when data is fluctuating above and below the threshold, and generating too many alerts. Initially, when an NAE-Lite agent is created, only the set-condition is active. Once the set-condition is met, the condition becomes inactive and the clear condition becomes active. The set-condition becomes active again once the clear condition is met.

The condition is met when any of the event logs watched by the **<WATCH-NAME>** has occurred and the event log message fits the include or exclude **<REGEX-LIST>** (if configured) and the condition has occurred for **<COUNT>** number of times (if configured).

The **no** form of this command removes the condition associated with the NAE-Lite agent.

Parameter	Description
<WATCH-NAME>	Specifies the name of the watch. This must be already defined using the watch command.
include {all any} <REGEX-LIST>	Configures the list of strings matching the regular expression that must be included in the event log message. Optional.
all	Includes all of the specified lists of regular expressions in event-log messages.
any	Includes any of the specified lists of regular expressions in event-log messages
<REGEX-LIST>	Specifies the comma-separated list of one or more regular expressions that must be matched against the event log messages. Optional.
exclude	Configures the list of strings matching the regular expression that must be included in the event log message. Optional.
count <COUNT>	Limits the number of times that the condition to be met once in every specified count. Optional. For example, if you want to monitor mac movement in the VLAN for every 10 th time, then the count must be specified as 10. Range: 1 to 4294967295.

Example

Defining the condition for the watch named **ipsla_status** including all the specified list:

```
switch(config-nae-agent) # set-condition watch event-log ipsla_status
include all "servername","failure" count 3
```

Clearing the condition for the watch named **ipsla_status** including all the specified list:

```
switch(config-nae-agent-condition) # clear-condition watch ipsla_status
include all "servername","success"
```

Defining the condition for the watch named **ipsla_status** excluding **snmpd**:

```
switch(config-nae-agent-condition) # set-condition watch event-log crash_event
exclude snmpd
```

Removing the conditions associated with the NAE-Lite agent:

```
switch(config-nae-agent) # no set-condition watch event-log ipsla_status include
all "servername","failure"
```

```
switch(config-nae-agent-condition) # no clear-condition watch ipsla_status
include all "servername","success"
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent config-nae-agent- condition	Administrators or local user group members with execution rights for this command.

show running-config nae-agent

```
show running-config nae-agent
```

Description

Shows the NAE-Lite agent current running configurations.

Example

Showing the NAE-Lite running configurations:

```

switch# show running-config nae-agent
Current configuration:
!
...
nae-agent lite memory_monitor
  desc Memory resource monitor
  monitor memory system memory line-module 1/3
  set-condition monitor memory gt 80
    status major
    syslog "High memory usage detected"
  cli show system
  clear-condition monitor memory lt 40
    status normal
    syslog "Memory usage is recovered to normal limit"

nae-agent lite crash_watch
  desc Watch the crash event
  tags crash, resource
  watch crash_event event-log 1201
  set-condition watch event-log crash_event
    status major
    cli show core-dump all
nae-agent lite crash_watch activate
nae-agent lite memory_monitor activate
...

```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

tags

```

tags <TAG-LIST>
no tags <TAG-LIST>

```

Description

Configures the tags applicable for the NAE-Lite agent. The tags are used to categorize and group the agent.

The **no** form of this command removes the tag lists associated with the NAE-Lite agent.

Parameter	Description
<code><TAG-LIST></code>	Specifies the tag list for the NAE-Lite agent. <code><TAG-LIST></code> is the comma separated list of tags. Each tag can be a minimum of 3 to a maximum of 32 characters in length. A maximum of 16 tags are supported.

Example

Configuring the tags for the NAE-Lite agent:

```
switch(config-nae-agent) # tags memory,resource,ztag
```

Removing the tags for the NAE-Lite agent:

```
switch(config-nae-agent) # no tags
```

```
switch(config-nae-agent) # no tags memory,resource
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent	Administrators or local user group members with execution rights for this command.

watch event-log

```
watch <WATCH-NAME> event-log <EVENT-ID-LIST>
no watch <WATCH-NAME> event-log <EVENT-ID-LIST>
```

Description

Configures the watch source for the NAE-Lite agent. This enables the agent to watch for specific events occurring in the system. Event-driven monitoring can be performed by watching the event log of the system.

For information on event IDs, refer to the Event Log Message Reference Guide.

The **no** form of this command removes the watch associated with the NAE-Lite agent.

Parameter	Description
<WATCH-NAME>	Specifies the watch name for the NAE-Lite agent. Length: 3 to 80 alphanumeric characters, including underscore (_).
<EVENT-ID-LIST>	Specifies the list of one or more event IDs of the event log message. A maximum of five event IDs can be specified.

Example

Configuring the watch source for the NAE-Lite agent.

```
switch(config-nae-agent) # watch crash_event event-log 1201
```

Removing the watch source used by the NAE-Lite agent:

```
switch(config-nae-agent) # no watch high_mem
```

```
switch(config-nae-agent) # no watch high_mem_event event-log 1208,1209
```



For more information on features that use this command, refer to the Network Analytics Engine Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-nae-agent	Administrators or local user group members with execution rights for this command.

switch config-validator

```
switch config-validator [config <CONFIG-NAME>] [feature <feature>] [mode {consistency |  
vsx-sync}] [format {cli | json}]
```

Description

Runs configuration validation to detect configuration anomalies.

Parameter	Description
config	Specifies configuration to be validated. The default configuration is running-config .
feature <feature>	Specifies the name of the feature to be validated.
mode	Specifies configuration validation mode. The default is consistency .
consistency	Validates feature configuration for consistency check.
vsx-sync	Validates VSX configuration synchronization between VSX peers for VSX enabled features.
format	Specifies the results display format. The default is cli .

Examples

Running configuration validation with switches for the vsx feature.

```
switch (config)# switch config-validator config running-config feature vsx  
Line number 36: Configuration `system-mac <VSX_SYSTEM_MAC>` is recommended  
Line number 36: Multi chassis configuration is recommended for VSX redundancy
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

arp ip mac

```
arp ip <IP-ADDR> mac <MAC-ADDR>
no arp ip <IP-ADDR> mac <MAC-ADDR>
```

Description

Configures static ARP multicast on the interface.

The **no** form of this command removes the static ARP multicast configuration.

Parameter	Description
<IP-ADDR>	Specifies cluster's virtual IPv4 address.
<MAC-ADDR>	Specifies multicast MAC address in IANA format (xx:xx:xx:xx:xx:xx) and non IANA format (xxxx.xxxx.xxxx).

Examples

Configuring static ARP multicast on an interface:

```
switch(config)# vlan 10
switch(config-vlan-10)# no shutdown
switch(config-vlan-10)# ip igmp snooping enable
switch(config-vlan-10)# exit
switch(config)# interface vlan10
switch(config-if-vlan)# ip igmp enable
switch(config-if-vlan)# arp ip 10.1.30.254 mac 01:00:5e:7f:1e:fe
```



If your NLB Virtual IP address is 10.1.30.254, then the server will join the 239.255.30.254 IGMP group. This IGMP group is mapped to the destination MAC address of 01:00:5e:7f:1e:fe.

On 8320, 8325/8325H/9325P, 9300/9300S, and 10000: The clusters sends the IGMP join to any valid multicast group IP address that is within the range from 224.0.0.0 to 239.255.255.255 except reserved group IP addresses.



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4

Release	Modification
	parameter is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if and config-if-vlan	Administrators or local user group members with execution rights for this command.

show arp

show arp

Description

Displays the static ARP multicast information.

Examples

Displaying the static ARP multicast information:

```
switch# show arp

IPv4 Address      MAC                Port              Physical Port    State
-----
3.3.3.3           01:00:5e:00:00:02          1/1/1            permanent
2.2.2.2           01:00:5e:00:00:01  vlan10            permanent

Total Number Of ARP Entries Listed- 2.
-----
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip igmp snooping vlan group

```
show ip igmp snooping vlan <VLAN-ID> group IGMP-Group
```

Description

Displays multicast joins (members of the cluster) participating in the IGMP group.

Examples

Displaying multicast joins participating in the IGMP group:

```
switch# show ip igmp snooping vlan 10 group 239.255.30.254

VLAN ID    : 10
VLAN Name  : VLAN10

Group Address : 239.255.30.254
Last Reporter : 10.1.30.254
Group Type   : Filter

Port      Vers Mode Uptime    Expires    V1      V2      Sources  Sources
-----  -  ---  -  -----  -  -----  -  -----
1/1/6     2    EXC  0m 21s   1m 12s     -      2m 48s   0        0
```

Displaying multicast joins participating in the IGMP group:

```
switch# show ip igmp snooping vlan 2 group 232.0.0.1

IGMP ports and group information for group 232.0.0.1

VLAN ID    : 2
VLAN Name  : VLAN2

Group Address : 232.0.0.1
Last Reporter : 30.1.1.1
Group Type   : Filter

Port      Vers Mode Uptime    Expires    V1      V2      Sources  Sources
-----  -  ---  -  -----  -  -----  -  -----
-
vxlan(5.5.5.5) 3    INC  14m 52s   0m 0s     -      -      1        0

Group Address: 232.0.0.1
Source Address: 30.1.1.30
Source Type:   Filter

Port      Mode Uptime    Expires    Configured Mode
-----  -  ---  -  -----  -
vxlan1(5.5.5.5) ING  14m 52s           Auto
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

ntp authentication

```
ntp authentication
no ntp authentication
```

Description

Enables support for authentication when communicating with an NTP server. The **no** form of this command disables authentication support.

Examples

Enabling authentication support:

```
switch(config)# ntp authentication
```

Disabling authentication support:

```
switch(config)# no ntp authentication
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ntp authentication-key

```
ntp authentication-key <KEY-ID> {md5 | sha1}
  [{ <PLAINTEXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
no ntp authentication-key <KEY-ID> {md5 | sha1}
  [{ <PLAINTEXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
```

Description

Defines an authentication key that is used to secure the exchange with an NTP time server. This command provides protection against accidentally synchronizing to a time source that is not trusted. The **no** form of this command removes the authentication key.

Parameter	Description
<code><KEY-ID></code>	Specifies the authentication key ID. Range: 1 to 65534.
<code>md5</code>	Selects MD5 key encryption.
<code>sha1</code>	Specifies SHA1 key encryption.
<code><PLAINTEXT-KEY></code>	Specifies the plaintext authentication key. Range: 8 to 40 characters. The key may contain printable ASCII characters excluding "#" or be entered in hex. Keys longer than 20 characters are assumed to be hex. To use an ASCII key longer than 20 characters, convert it to hex.
<code>trusted</code>	Specifies that this is a trusted key. When NTP authentication is enabled, the switch only synchronizes with time servers that transmit packets containing a trusted key.
<code>ciphertext <ENCRYPTED-KEY></code>	Specifies the ciphertext authentication key in Base64 format. This is used to restore the NTP authentication key when copying configuration files between switches or when uploading a previously saved configuration. NOTE: When the key is not provided on the command line, plaintext key prompting occurs upon pressing Enter, followed by prompting as to whether the key is to be trusted. The entered key characters are masked with asterisks.

Examples

Defining key 10 with MD5 encryption and a provided plaintext trusted key:

```
switch(config)# ntp authentication-key 10 md5 F82#450b trusted
```

Defining key 5 with SHA1 encryption and a prompted plaintext trusted key:

```
switch(config)# ntp authentication-key 5 sha1
Enter the NTP authentication key: *****
Re-Enter the NTP authentication key: *****

Configure the key as trusted (y/n)? y
```

Removing key 10:

```
switch(config)# no ntp authentication-key 10
```




For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ntp disable

ntp disable

Description

Disables the NTP client on the switch. The NTP client is disabled by default.

Examples

Disabling the NTP client.

```
switch(config)# ntp disable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ntp enable

ntp enable

```
no ntp enable
```

Description

Enables the NTP client on the switch to automatically adjust the local time and date on the switch. The NTP client is disabled by default.

The **no** form of this command disables the NTP client.

Examples

Enabling the NTP client.

```
switch(config)# ntp enable
```

Disabling the NTP client.

```
switch(config)# no ntp enable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ntp conductor

```
ntp conductor vrf <VRF-NAME> {stratum <NUMBER>}  
no ntp conductor vrf <VRF-NAME> {stratum <NUMBER>}
```

Description

Sets the switch as the conductor time source for NTP clients on the specified VRF. By default, the switch operates at stratum level 8. The switch cannot function as both NTP conductor and client on the same VRF.

The **no** form of this command stops the switch from operating as the conductor time source on the specified VRF.

Parameter	Description
<code>vrf <VRF-NAME></code>	Specifies the VRF on which to act as conductor time source.
<code>stratum <NUMBER></code>	Specifies the stratum level at which the switch operates. Range: 1 - 15. Default: 8.

Examples

Setting the switch to act as conductor time source on VRF **primary-vrf** with a stratum level of **9**.

```
switch(config)# ntp conductor vrf primary-vrf stratum 9
```

Stops the switch from acting as conductor time source on VRF **primary-vrf**.

```
switch(config)# no ntp conductor vrf primary-vrf
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.08	Inclusive language.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ntp server

```
ntp server <IP-ADDR> [key <KEY-NUM>] [minpoll <MIN-NUM>] [maxpoll <MAX-NUM>] [burst |
iburst] [prefer] [version <VER-NUM>]
no ntp server <IP-ADDR> <IP-ADDR> [key <KEY-NUM>] [minpoll <MIN-NUM>] [maxpoll <MAX-NUM>]
[burst | iburst] [prefer] [version <VER-NUM>]
```

Description

Defines an NTP server to use for time synchronization, or updates the settings of an existing server with new values. Up to eight servers can be defined.

The **no** form of this command removes a configured NTP server.



The default NTP version is 4; it is backwards compatible with version 3.

Parameter	Description
<code>server <IP-ADDR></code>	Specifies the address of an NTP server as a DNS name, an IPv4 address (x.x.x.x), where x is a decimal number from 0 to 255, or an IPv6 address (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. When specifying an IPv4 address, you can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100 . When specifying an IPv6 address, you can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
<code>key <KEY-NUM></code>	Specifies the key to use when communicating with the server. A trusted key must be defined with the command ntp authentication-key and authentication must be enabled with the command ntp authentication . Range: 1 to 65534.
<code>minpoll <MIN-NUM></code>	Specifies the minimum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 6 (64 seconds).
<code>maxpoll <MAX-NUM></code>	Specifies the maximum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 10 (1024 seconds).
<code>burst</code>	Send a burst of packets instead of just one when connected to the server. Useful for reducing phase noise when the polling interval is long.
<code>iburst</code>	Send a burst of six packets when not connected to the server. Useful for reducing synchronization time at startup.
<code>prefer</code>	Make this the preferred server.
<code>version <VER-NUM></code>	Specifies the version number to use for all outgoing NTP packets. Range: 3 or 4. Default: 4.
	NOTE: NTP is backwards compatible.

Usage

For features such as Activate and ZTP, a switch that has a factory default configuration will automatically be configured with pool.ntp.org. NTP server configurations via DHCP options are supported. The DHCP server can be configured with maximum of two NTP server addresses which will be supported on the switch. Only IPV4 addresses are supported.



When configuring a time backward more than five minutes on the HPE Aruba Networking 8320, 8325, or 9300 Switch Series, a reboot is recommended to avoid unusual switch behavior.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as a radio or atomic clock or a GPS time source).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 time server.

When using multiple servers with same stratum setting, the best practice to configure a preferred server, so NTP will attempt to use the preferred server as the primary NTP connection. If a preferred server is not manually set when NTP is enabled, the configured server with the lowest stratum will automatically be set as the preferred server. If there are servers with the same stratum, this auto prefer status will prevent AOS-CX from toggling between different servers as the primary server. Auto prefer selection of servers with same stratum (if not manually selected) may change after reconfiguring the switch, or after executing the **reboot** command.

Examples

Defining the ntp server pool.ntp.org, using iburst, and NTP version 4.

```
switch(config)# ntp server pool.ntp.org iburst version 4
```

Removing the ntp server pool.ntp.org.

```
switch(config)# no ntp server pool.ntp.org
```

Defining the ntp server my-ntp.mydomain.com and makes it the preferred server.

```
switch(config)# ntp server my-ntp.mydomain.com prefer
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ntp trusted-key

```
ntp trusted-key <KEY-ID>  
no ntp trusted-key <KEY-ID>
```

Description

Sets a key as trusted. When NTP authentication is enabled, the switch only synchronizes with time servers that transmit packets containing a trusted key.

The **no** form of this command removes the trusted designation from a key.

Parameter	Description
<KEY-ID>	Specifies the identification number of the key to set as trusted. Range: 1 to 65534.

Examples

Defining key 10 as a trusted key.

```
switch(config)# ntp trusted-key 10
```

Removing trusted designation from key 10:

```
switch(config)# no ntp trusted-key 10
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ntp vrf

```
ntp vrf <VRF-NAME>
no ntp vrf <VRF-NAME>
```

Description

Specifies the VRF on which the NTP client communicates with an NTP server. The switch cannot function as both NTP conductor and client on the same VRF.

The **no** form of the command returns to default VRF.

Parameter	Description
<VRF-NAME>	Specifies the name of a VRF.

Example

Setting the switch to use the default VRF for NTP client traffic.

```
switch(config) # ntp vrf default
```

Setting the switch to use the default management VRF for NTP client traffic.

```
switch(config) # ntp vrf mgmt
```

Returning the switch to use the default VRF for NTP client traffic.

```
switch(config) # no ntp vrf
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show ntp associations

```
show ntp associations [vsx-peer]
```

Description

Shows the status of the connection to each NTP server. The following information is displayed for each server:

- Tally code : The first character is the Tally code:
 - (blank): No state information available (e.g. non-responding server)
 - x : Out of tolerance (discarded by intersection algorithm)
 - . : Discarded by table overflow (not used)
 - - : Out of tolerance (discarded by the cluster algorithm)
 - + : Good and a preferred remote peer or server (included by the combine algorithm)
 - # : Good remote peer or server, but not utilized (ready as a backup source)
 - * : Remote peer or server presently used as a primary reference
 - o : PPS peer (when the prefer peer is valid)
- ID: Server number.
- NAME: NTP server FQDN/IP address (Only the first 24 characters of the name are displayed).

- REMOTE: Remote server IP address.
- REF_ID: Reference ID for the remote server (Can be an IP address).
- ST: (Stratum) Number of hops between the NTP client and the reference clock.
- LAST: Time since the last packet was received in seconds unless another unit is indicated.
- POLL: Interval (in seconds) between NTP poll packets. Maximum (1024) reached as server and client sync.
- REACH: 8-bit octal number that displays status of the last eight NTP messages (377 = all messages received).

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show ntp associations
-----
ID           NAME           REMOTE           REF-ID ST LAST POLL REACH
-----
1           192.0.1.1       192.0.1.1       .INIT. 16   -   64    0
* 2  time.apple.com  17.253.2.253    .GPSs.  2   70  128   377
-----
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ntp authentication-keys

`show ntp authentication-keys [vsx-peer]`

Description

Shows the currently defined authentication keys.

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show ntp authentication-keys
-----
Auth key  Trusted  MD5 password
-----
10        No      *****
20        Yes     *****
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ntp servers

`show ntp servers[vsx-peer]`

Description

Shows all configured NTP servers, including any DHCP servers, default pool servers or any server with the status **auto prefer**.

Parameter	Description
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show ntp servers
-----
      NTP SERVER KEYID MINPOLL MAXPOLL OPTION VER
-----
      192.0.1.18      -      5      10 iburst   3
      192.0.1.19      -      6      10  none    4
      192.0.1.20      -      6       8  burst   3 prefer
-----
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ntp statistics

```
show ntp statistics [vsx-peer]
```

Description

Shows global NTP statistics. The following information is displayed:

- Rx-pkts: Total NTP packets received.
- Current Version Rx-pkts: Number of NTP packets that match the current NTP version.
- Old Version Rx-pkts: Number of NTP packets that match the previous NTP version.
- Error pkts: Packets dropped due to all other error reasons.
- Auth-failed pkts: Packets dropped due to authentication failure.
- Declined pkts: Packets denied access for any reason.
- Restricted pkts: Packets dropped due to NTP access control.
- Rate-limited pkts: Number of packets discarded due to rate limitation.
- KOD pkts: Number of Kiss of Death packets sent.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch(config)# show ntp statistics
Rx-pkts 100
Current Version Rx-pkts 80
Old Version Rx-pkts 20
Err-pkts 2
Auth-failed-pkts 1
Declined-pkts 0
Restricted-pkts 0
Rate-limited-pkts 0
KoD-pkts 0
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ntp status

```
show ntp status [vsx-peer]
```

Description

Shows the status of NTP on the switch.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying the status information when the switch is not synced to an NTP server:

```
switch# show ntp status
NTP is enabled.
NTP authentication is enabled.
```

```
NTP is using the default VRF for NTP server connections.
```

```
Wed Nov 23 23:29:10 PDT 2016  
NTP uptime: 187 days, 1 hours, 37 minutes, 48 seconds
```

```
Not synchronized with an NTP server.
```

Displaying the status information when the switch is synced to an NTP server:

```
switch# show ntp status  
NTP is enabled.  
NTP authentication is enabled.  
NTP is using the default VRF for NTP server connections.
```

```
Wed Nov 23 23:29:10 PDT 2016  
NTP uptime: 187 days, 1 hours, 37 minutes, 48 seconds
```

```
Synchronized to NTP Server 17.253.2.253 at stratum 2.  
Poll interval = 1024 seconds.  
Time accuracy is within 0.994 seconds  
Reference time: Thu Jan 28 2016 0:57:06.647 (UTC)
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

active-backbone

```
active-backbone stub-default-route  
no active-backbone stub-default-route
```

Description

This command enables the router to send a default route to stub areas if there is an active loopback link in the backbone area. The configuration is not required if backbone area has neighbors or passive interfaces configured. By default active backbone detection is enabled.

Examples

```
switch(config)# router ospf 1  
switch(config-ospf-1)# active-backbone stub-default-route
```

```
switch(config)# no active-backbone stub-default-route
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10.1000	Command Introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf- <i><PROCESS-ID></i> config-ospfv3- <i><PROCESS-ID></i>	Administrators or local user group members with execution rights for this command.

area (ospf)

```
area <AREA-ID>  
no area <AREA-ID>
```

Description

Creates a normal area, with *<AREA-ID>* set if not present. If the area is already present and it is not a normal area, then this command changes the area type to normal.

The **no** form of this command deletes the area with the **<AREA-ID>** specified. Area can be of any type (nssa, nssa no-summary, stub, stub no-summary, and default normal area).

Parameter	Description
<AREA-ID>	Specifies the area ID in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.

Examples

Creating a normal area:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 1
switch(config-ospf-1)# area 10.1.1.1
Switch(config-ospf-1)# show running-config current-context router ospf 1
    router-id 1.1.1.1
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2 stub
    area 0.0.0.3 nssa
```

Deleting an area:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no area 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area default-metric

```
area <AERA-ID> default-metric <COST>
no area <AREA-ID> default-metric
```

Description

Sets the cost of the default route announced to NSSA or stub areas.

The **no** form of this command resets the cost of the default route announced to NSSA or stub areas, to the default value of 1.

Parameter	Description
<code><AREA-ID></code>	Specifies area ID in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
<code>default-metric <COST></code>	Sets the cost of default-summary LSAs announced to NSSA or stub areas, to the specified value. Default cost: 1. Range: 0 to 16777215.

Examples

Setting cost for default LSA summary:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 1 default-metric 2
switch(config-ospf-1)# area 0.0.0.1 default-metric 2
```

Setting cost for default LSA summary to default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no area 1 default-metric
switch(config-ospf-1)# no area 0.0.0.1 default-metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospf-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

area nssa

```
area <AREA-ID> nssa [no-summary]
no area <AREA-ID> nssa [no-summary]
```

Description

Creates the NSSA area (Not So Stubby Area) with **<AREA-ID>** if not present. If area is present and not NSSA area, this command changes the area type to NSSA area. If **no-summary** is used, area type will be NSSA No-Summary.

The **no** form of this command unsets the area type as NSSA. That is, the configured area will be changed to default normal area. The **no area <AREA-ID> nssa no-summary** command enables sending inter-area routes into NSSA, but will not unset the area as NSSA.

Parameter	Description
<code><AREA-ID></code>	Specifies the area ID in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
<code>nssa [no-summary]</code>	Specifies Not So Stubby Area (NSSA) area type. If area is present and not NSSA area, parameter changes the area type to NSSA area. If no-summary is specified, area type will be NSSA No-Summary, which means do not inject inter-area routes into NSSA.

Examples

Creating an NSSA area:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 1 nssa
switch(config-ospf-1)# area 1 nssa no-summary
```

Unsetting the area as NSSA

```
switch(config)# router ospf 1
switch(config-ospf-1)# no area 1 nssa
switch(config-ospf-1)# no area 1 nssa no-summary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospf-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

area range


```
area <AREA-ID> range <IP-PREFIX> type {inter-area | nssa} [no-advertise]
no area <AREA-ID> range <IP-PREFIX> type {inter-area | nssa} [no-advertise]
```

Description

Summarizes the routes with the matching address or masks. This command only works for border routers.

The **no** form of this command removes route summarization for the configured IPv4 prefix address on the ABR. When using the **no** form of the command with the **no-advertise** option, enables advertising this range to other areas.

Parameter	Description
<AREA-ID>	Specifies the area ID in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
range <IP-PREFIX>	Specifies summarizing routes matching the area range prefix/mask.
type {inter-area nssa}	Specifies the type this address aggregation applies to as either inter-area range prefix or NSSA range prefix.
no-advertise	Specifies the address range status as DoNotAdvertise (do not advertise this range to other areas).

Examples

Summarizing inter-area or NSSA paths:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 1
switch(config-ospf-1)# area 2 nssa
switch(config-ospf-1)# area 1 range 192.77.114.0/24 type inter-area
switch(config-ospf-1)# area 2 range 192.77.114.0/24 type nssa
switch(config-ospf-1)# area 2 range 192.77.114.0/24 type nssa no-advertise
```

Removing summarization:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no area 1 range 192.77.114.0/24 type inter-area
switch(config-ospf-1)# no area 2 range 192.77.114.0/24 type nssa
switch(config-ospf-1)# no area 2 range 192.77.114.0/24 type nssa no-advertise
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area stub

```
area <AREA-ID> stub [no-summary]
no area <AREA-ID> stub [no-summary]
```

Description

Creates the stub area with <AREA-ID> if not present. If the area is already present and it is not a normal stub area, then this command changes the stub area type to normal. If the **no-summary** parameter is used, area type will be stub No-Summary.

The **no** form of this command unsets the area as a stub type. That is, the configured area will be changed to a default normal area. The **no area <AREA-ID> stub no_summary** command enables sending inter-area routes into the stub area, but will not unset the area as stub.



ABR does not inject the default route in a Totally Stubby Area with loopback in Area 0.0.0.0. As a workaround, configure a passive interface or active neighbors in the backbone area.

Parameter	Description
<AREA-ID>	Specifies the area ID in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
stub [no-summary]	Specifies the stub area type. If the area is already present and it is not a stub area, this parameter changes the area type to stub. If no-summary is specified, area type will be stub No-Summary (totally stubby area), which means do not inject summary link advertisements into stub areas.

Examples

Creating a STUB area:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 1 stub
switch(config-ospf-1)# area 1 stub no-summary
```

Unsetting the area type as stub:

```
switch(config)# router ospf 1
switch(config-ospf-1) # no area 1 stub
switch(config-ospf-1) # no area 1 sub no-summary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area virtual-link

```
area <AREA-ID> virtual-link <ROUTER-ID>
no area <AREA-ID> virtual-link <ROUTER-ID>
```

Description

Creates an OSPF virtual link with a remote ABR and enters the vlink context.

The **no** form of this command deletes an OSPF virtual link with the specified router ID of the remote ABR. If no **<ROUTER-ID>** is specified, the **no** form of the command sets the virtual link to the default settings.

Parameter	Description
<AREA-ID>	Specifies the area ID in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
virtual-link <ROUTER-ID>	Configures a virtual link with the specified router ID of the remote ABR.

Examples

Configuring OSPF virtual links:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)#
```

Deleting OSPF virtual links:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no area 100 virtual-link 100.0.1.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

authentication

```
authentication {hmac-sha-1 | hmac-sha-256 | hmac-sha-384 | hmac-sha-512 | message-digest  
| simple-text | null | keychain}  
no authentication
```

Description

Sets the OSPF virtual-link authentication type that will be used for authentication with the remote ABR. Choose one of the authentication types from the following parameters.

The **no** form of this command unconfigures the virtual-link authentication type used and sets it to Null authentication.

Parameter	Description
hmac-sha-1	Sets the authentication type as SHA-1.
hmac-sha-256	Sets the authentication type as SHA-256.
hmac-sha-384	Sets the authentication type as SHA-384.
hmac-sha-512	Sets the authentication type as SHA-512.
message-digest	Sets the authentication type to message-digest.
simple-text	Sets the authentication type to simple-text.
null	Sets the authentication type to null.
keychain	Sets authentication type to use the key chain.

Examples

Setting OSPF virtual links authentication type:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# authentication simple-text
```

Deleting OSPF virtual links authentication type:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# no authentication
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

authentication-key

```
authentication-key [{ciphertext | plaintext} <PASSWORD>]  
no authentication-key
```

Description

Sets the OSPF virtual-link authentication password that is used for simple-text authentication. If the password is given in ciphertext, it will be decrypted and applied to the protocol.

The **no** form of this command deletes the virtual-link authentication password that is used for simple-text authentication.

Parameter	Description
{ciphertext plaintext}	Selects the password format.
<PASSWORD>	Specifies the password.



When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Setting the OSPF virtual link simple-text authentication password in plaintext format:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# authentication-key plaintext F82#450b
```

Setting the OSPF virtual link simple-text authentication with a prompted plaintext password:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# authentication-key  
Enter the authentication key: *****  
Re-Enter the authentication key: *****
```

Setting the OSPF virtual link simple-text authentication password in ciphertext format:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# authentication-key ciphertext AQaAz05...RmH+4pg=
```

Deleting the OSPF virtual link simple-text authentication password:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# no authentication-key
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

clear ip ospf neighbors

```
clear ip ospf [<PROCESS-ID>] neighbor [<NEIGHBOR>] [interface [<INTERFACE-NAME>]]  
[all-vrfs | vrf <VRF-NAME>]
```

Description

Resets the neighbor and clears the OSPF neighbor information.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv2 process ID to clear the statistics for the particular OSPFv2 process. Range: 1 to 65535.
<NEIGHBOR>	Specifies the router ID of a neighbor.
<INTERFACE-NAME>	Specifies the OSPFv2 statistics to clear for the specified interface.
all-vrfs	Select to clear the OSPFv2 statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv2 neighbor information:

```
switch# clear ip ospf 1 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf 1 neighbor 1.1.1.2
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf 1 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf 1 neighbor 1.1.1.5 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf neighbor 1.1.1.4
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ip ospf neighbor 1.1.1.5 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear ip ospf statistics

clear ip ospf [<PROCESS-ID>] statistics [interface [<INTERFACE-NAME>]] [all-vrfs | vrf <VRF-NAME>]

Description

Clear the OSPF event statistics.

Parameter	Description
<PROCESS-ID>	OSPF process ID. Clear the statistics for the particular OSPF process. Range: 1 to 65535.
<INTERFACE-NAME>	Clear the OSPF statistics for the specified interface.
all-vrfs	Optionally select to clear the OSPF statistics for all VRFs.
vrf <VRF-NAME>	Optionally select to clear the OSPF statistics for a particular VRF. If the VRF is not specified, information for the default VRF is cleared.

Examples

Clearing the OSPF event statistics:

```
switch# clear ip ospf statistics
switch# clear ip ospf statistics interface 1/1/1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

dead-interval

```
dead-interval <INTERVAL>
no dead-interval
```

Description

Sets the interval after which a neighbor is declared dead if no hello packet comes in for virtual links. The **no** form of this command sets the dead interval to default for virtual links. The default value is 40 seconds (generally four times the hello packet interval).



For proper operation, set the dead interval must be longer than the hello interval.

Parameter	Description
<INTERVAL>	Specifies the time interval for the dead interval, in seconds. Range: 1 to 65535. Default: 40.

Examples

Setting the OSPv2F virtual links dead interval:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# dead-interval 30
```

Setting the OSPFv2 virtual links dead interval to default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# no dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

default-information originate

```
default-information originate [metric <METRIC-VALUE>]
no default-information originate [metric <METRIC-VALUE>]
```

Description

Configures OSPF to advertise the default route (0.0.0.0/0) to its neighbors if it is present in the routing table. Optionally, the metric value can be set for default route ::/0. The default value is 1.

The **no** form of this command disables advertisement of the default route.

Parameter	Description
<code>metric <METRIC-VALUE></code>	Specifies the OSPF metric value for the default route. Optional. Default: 1.

Examples

Setting advertisement of the default route:

```
switch(config)# router ospf 1
switch(config-ospf-1)# default-information originate
```

Disabling advertisement of the default route:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no default-information originate
```

Setting advertisement of the default route and specifying an optional metric value of 20:

```
switch(config)# router ospf 1
switch(config-ospfv3-1)# default-information originate
switch(config-ospfv3-1)# default-information originate metric 20
```

Disabling advertisement of the default route and setting metric to the default value:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no default-information originate metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Added parameter: metric <METRIC-VALUE>
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospf-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

default-information originate always

default-information originate always [metric <METRIC-VALUE>]
no default-information originate always [metric <METRIC-VALUE>]

Description

Configures OSPF to advertise the default route (0.0.0.0/0) to its neighbors, regardless if it is present in the routing table or not. Optionally, metric can be set for default route 0.0.0.0/0. The default value is 1. The **no** form of this command disables advertisement of the default route.

Parameter	Description
<code>metric <METRIC-VALUE></code>	Specifies the OSPF metric value for the default route. Default: 1.

Examples

Setting advertisement of the default route:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# default-information originate always
```

Disabling advertisement of the default route:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# no default-information originate always
```

Setting advertisement of the default route with metric set to 20:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# default-information originate always metric 20
```

Disabling advertisement of the default route and setting the metric to the default value:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# no default-information originate always metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Added parameter: metric <METRIC-VALUE>
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

default-metric

```
default-metric <METRIC-VALUE>
no default-metric
```

Description

Sets the default metric for redistributed routes in the OSPF.

The **no** form of this command sets the default metric to be used for redistributed routes into OSPF to the default of 25.

Parameter	Description
<METRIC-VALUE>	Specifies the default metric value to use for redistributed routes. Default: 25. Range: 0-1677214.

Examples

Setting default metric for redistributed routes:

```
switch(config)# router ospf 1
switch(config-ospf-1)# default-metric 37
```

Setting default metric for redistributed routes to the default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no default-metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables the OSPF process.



This command does not remove the OSPF configurations.

Examples

Disabling OSPF process:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

distance

```
distance [<DISTANCE-VAL> | intra-area [<DISTANCE-VAL>] | inter-area [<DISTANCE-VAL>] |  
external [<DISTANCE-VAL>]]  
no distance [intra-area | inter-area | external]
```

Description

Defines an Administrative Distance (AD) for OSPF. Administrative Distance is used as a criteria to select the best route when multiple routes are present from different routing protocols.

The **no** form of this command sets the OSPF administrative distance to the default of 110. Optionally, administrative distance can be set to default for the specific OSPF route type: intra-area, inter-area, or external type-5 and type-7 routes.

Parameter	Description
<DISTANCE-VAL>	Specifies the OSPF administrative distance. Range: 1 to 255. Default: 110.
intra-area	Specifies the OSPF distance for intra-area routes.

Parameter	Description
inter-area	Specifies the OSPF distance for inter-area routes.
external	Specifies the OSPF distance for external type 5 and type 7 routes.

Usage

Within a given OSPF process, intra-area routes are always given precedence even when distances are configured for inter-area or external type routes.

Examples

Setting OSPF administrative distance:

```
switch(config)# router ospf 1
switch(config-ospf-1)# distance 100
switch(config-ospf-1)# distance intra-area 24 external 55 inter-area 66
switch(config-ospf-1)# distance intra-area 24 external 55
switch(config-ospf-1)# distance external 55
switch(config-ospf-1)#exit

switch(config)# router ospf 2
switch(config-ospf-2)# distance 200
switch(config-ospf-2)# distance external 60
switch(config-ospf-2)# distance intra-area 24 inter-area 66
```

Setting OSPF administrative distance to the default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no distance
switch(config-ospf-1)# no distance external
switch(config-ospf-1)# no distance inter-area
switch(config-ospf-1)# no distance intra-area
switch(config-ospf-1)# no distance 100
switch(config-ospf-1)# no distance 220

switch(config)# router ospf 2 vrf blue
switch(config-ospf-2)# no distance 200
switch(config-ospf-2)# no distance external 60
switch(config-ospf-2)# no distance intra-area 24 inter-area 66
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Added capability to have individual admin distance for multiple OSPF processes in a VRF.
10.09	Added parameters: intra-area , inter-area , external
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

distribute-list prefix

```
distribute-list prefix <prefix-list-name> {in | out}  
no distribute-list prefix <prefix-list-name> {in | out}
```

Description

This command uses an existing prefix list to filter routes that are being installed in the routing table or redistributed to another routing protocol.

The **distribute-list prefix** command filters routes in the inbound or the outbound direction. When this command is issued with the **in** parameter, it filters routes from being installed in the routing table, it does not filter LSAs. When this command is issued with the **out** parameter, it filters only the desired redistributed routes from other protocols.



This command requires that your prefix list is already defined using the [ip prefix](#) commands. Route-maps are not supported with the distribute-list feature.

Parameter	Description
prefix <prefix-list-name>	Specify the name of an existing prefix.
{in out}	Select one of the following parameters to set the filter direction: ▪ in: Filter incoming routes into the routing table ▪ out: Filter outgoing routing updates

Examples

The following commands enable the filtering of OSPFv2 routes in an IPv4 network, so routes are no longer installed in the routing table or redistributed from another routing protocol.

```
switch(config)# router ospfv2 1  
switch(config-ospfv2-1)# distribute-list prefix listA in  
switch(config-ospfv2-1)# distribute-list prefix listB out
```

The following command disables the filtering of OSPFv2 routes in an IPv4 network, so routes can be installed in the routing table or redistributed from another routing protocol.

```
switch# configure terminal  
switch(config)# router ospfv2 1  
switch(config-ospfv2-1)# no distribute-list prefix listA in  
switch(config-ospfv2-1)# no distribute-list prefix listB out
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv2-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables the OSPF process, if disabled. By default the OSPF process is enabled.

Examples

Enabling OSPF process:

```
switch(config)# router ospf 1
switch(config-ospf-1)# enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

graceful-restart

```
graceful-restart
restart-interval <INTERVAL>
helper [strict-lsa-check]
ignore-lost-interface
no...
```

Description

Configures graceful restart parameters for OSPF.

The **no** form of this command sets the restart interval to the default interval of 120 seconds or disables the helper mode, depending on the parameter specified.

Parameter	Description
<code>restart-interval <INTERVAL></code>	Specifies the time another router waits for this router to gracefully restart and selects the maximum time to wait in seconds. Range: 5 to 1800. Default: 120.
<code>helper</code>	Specifies that the router will participate in the graceful restart of a neighbor router.
<code>strict-lsa-check</code>	(Optional). Use with the helper parameter to enable strict Link state Advertisement (LSA) checking when acting as a restart helper for a restarting peer. NOTE: OSPF neighbors must disable strict LSA checking. If the local node has fewer OSPF interfaces after restarting, then the neighbors that were adjacent on those interfaces will clear up their adjacencies to the restarting node and will send out link state updates to advertise the dropped adjacency. If strict LSA checking is enabled, the restarting router's neighbors will exit helper mode when they receive the updated LSAs and the graceful restart will still fail.
<code>ignore-lost-interface</code>	Enable the restarting router to ignore lost OSPF interfaces during a graceful restart process. This setting should be enabled on a high availability system to ensure a graceful restart completes successfully, even if OSPF-enabled links fail due to High Availability events like a switchover or failover. NOTE: Enabling this setting means that the hitless restart procedures do not strictly follow those defined in <i>RFC 3623, Graceful OSPF Restart</i> .
<code>no</code>	Negate any parameter or return the setting to its default.

Examples

Enabling OSPF graceful restart:

```
switch(config)# router ospf 1
switch(config-ospf-1)# graceful-restart restart-interval 40
switch(config-ospf-1)# graceful-restart helper strict-lsa-check
```

Enabling the switch to ignore lost OSPF interfaces during a graceful restart process:

```
switch(config)# router ospf 1
switch (config-ospf-1)# graceful-restart ignore-lost-interface
```

Setting the restart interval to default, and disabling helper mode:

```
switch(config)# router ospf 1
switch(config-ospfv3-1)# no graceful-restart restart-interval
switch(config-ospfv3-1)# no graceful-restart helper
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

hello-interval

```
hello-interval <INTERVAL>
no hello-interval
```

Description

Sets the time interval between OSPF hello packets for virtual links.

The **no** form of this command sets the hello interval to the default value of 10 seconds for virtual links.



For proper operation, the hello interval must be shorter than the dead interval.

Parameter	Description
<INTERVAL>	Specifies the time interval for the hello interval, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting the OSPF virtual links hello interval:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# hello-interval 30
```

Setting the OSPF virtual links hello interval to default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# no hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

ip ospf area

```
ip ospf <PROCESS-ID> area <AREA-ID>
no ip ospf <PROCESS-ID> area <AREA-ID>
```

Description

Runs the OSPF protocol on the interface with the configured IPv4 address for the area specified. The interfaces which have an IP address configured in this network or in a subset of this network, will participate in the OSPF protocol.

To move an interface to a new area, unmap the existing area and then associate a new area with the interface.

The **no** form of this command disables OSPF on the interface and removes the interface from the area. Interfaces which have an IP address configured on the network or in a subset of the network, stop participating in the OSPF protocol.

Parameter	Description
<PROCESS-ID>	Specifies the OSPF process Id. Range: 1 to 65535.
<AREA-ID>	Specifies the OSPF area ID in one of the following formats. Area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Area identifier in decimal format. Range: 0 to 4294967295.

Examples

Setting OSPF network for the area:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf 1 area 1
switch(config-if-vlan)# ip ospf 1 area 0.0.0.1
```

Disabling OSPF network for the area:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf 1 area 1
switch(config-if-vlan)# no ip ospf 1 area 0.0.0.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf authentication

```
ip ospf authentication {message-digest | simple-text | null | keychain | hmac-sha-1 |  
hmac-sha-256 | hmac-sha-384 | hmac-sha-512}  
no ip ospf authentication
```

Description

Sets the authentication type that will be used for authentication with the neighbor router.

The **no** form of this command deletes the authentication type used for a particular authentication with the neighbor router and sets to null authentication.

Parameter	Description
message-digest	Sets authentication type as message-digest.
simple-text	Sets authentication type as simple-text.
null	Sets authentication type as null.
keychain	Sets the authentication type to use the key chain.
hmac-sha-1	Sets the authentication type to SHA-1.
hmac-sha-256	Sets the authentication type to SHA-256.
hmac-sha-384	Sets the authentication type to SHA-384.
hmac-sha-512	Sets the authentication type to SHA-512.

Examples

Setting OSPF authentication type on the interface:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# ip ospf authentication simple-text
```

Deleting OSPF authentication type on the interface and sets it to null:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf authentication
```

Setting OSPF authentication type to SHA-384 on the interface:

```
switch(config)# interface vlan 5
switch(config-if-vlan)# ip ospf authentication hmac-sha-384
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip ospf authentication-key

```
ip ospf authentication-key [{ciphertext | plaintext} <PASSWORD>]
no ip ospf authentication-key
```

Description

Sets the authentication password used for simple-text authentication. If the password is given in ciphertext it will be decrypted and applied to the protocol.

The **no** form of this command deletes the authentication password used for simple-text authentication.

Parameter	Description
{ciphertext plaintext}	Selects the password format.
<PASSWORD>	Specifies the password.



When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Setting the OSPF simple-text authentication password in plaintext format:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf authentication-key plaintext F82#450b
```

Setting the OSPF simple-text authentication password with a prompted plaintext password:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf authentication-key
Enter the authentication key: *****
Re-Enter the authentication key: *****
```

Setting the OSPF simple-text authentication password in ciphertext format:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf authentication-key ciphertext AQBaZ...ecopg=
```

Deleting the OSPF simple-text authentication password:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf authentication-key
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf cost

```
ip ospf cost <INTERFACE-COST>
no ip ospf cost
```

Description

Sets the cost (metric) associated with a particular interface. The interface cost is used as a parameter to calculate the best routes.

The **no** form of this command sets the cost (metric) associated with a particular interface to the default cost 1.

Parameter	Description
<INTERFACE-COST>	Specifies the interface cost value. Range: 1 to 65535. Default: 1.

Examples

Setting OSPF interface cost

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf cost 100
```

Setting the OSPF interface cost to default

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf cost
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	

ip ospf dead-interval

```
ip ospf dead-interval <INTERVAL>
no ip ospf dead-interval
```

Description

Sets the interval after which a neighbor is declared dead if no hello packet is received on the OSPF interface.

The **no** form of this command sets the interval after which a neighbor is declared dead, to the default for the OSPF interface. The default value is 40 seconds (generally 4 times the hello packet interval).

Parameter	Description
<INTERVAL>	Specifies the time interval for the dead interval, in seconds. Range: 1 to 65535. Default: 40.

Examples

Setting OSPF dead interval on the interface:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# ip ospf dead-interval 30
```

Setting OSPF dead interval to default on the interface:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# no ip ospf dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf hello-interval

```
ip ospf hello-interval <INTERVAL>  
no ip ospf hello-interval
```

Description

Sets the time interval between OSPF hello packets for the OSPF interface.

The **no** form of this command sets the time interval OSPF hello packets to the default of 10 seconds for the OSPF interface.

Parameter	Description
<INTERVAL>	Specifies the time interval for the hello interval, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting OSPF hello interval on the interface:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# ip ospf hello-interval 30
```

Setting OSPF hello interval to the default on the interface:


```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf keychain

```
ip ospf keychain <KEYCHAIN-NAME>
no ip ospf keychain
```

Description

Sets the key chain for md5 authentication. A key chain configures rotating keys for packet authenticating, reducing the risk of keys being compromised.

The **no** form of this command deletes the key chain used for md5 authentication.

Parameter	Description
<KEYCHAIN-NAME>	Name of key chain to be used for md5 authentication.

Examples

Setting OSPFv2 key chain authentication:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf keychain ospf_keys
```

Deleting OSPFv2 key chain authentication:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip ospf keychain
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip ospf message-digest-key md5

```
ip ospf message-digest-key <KEY-ID> md5 [{ciphertext | plaintext} <KEY>]
no ip ospf message-digest-key <KEY-ID>
```

Description

Sets the md5 message digest authentication key. If the md5 key is given in ciphertext, it will be decrypted and applied to the protocol.

The **no** form of this command deletes the md5 authentication key.

Parameter	Description
<KEY-ID>	Specifies the md5 key ID. Range: 1 to 255.
{ciphertext plaintext}	Selects the md5 key format.
<KEY>	Specifies the md5 authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting the md5 key in plaintext format:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf message-digest-key 1 md5 plaintext F82#450b
```

Setting the md5 key with a prompted plaintext key:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf message-digest-key 1 md5
Enter the MD5 authentication key: *****
Re-Enter the MD5 authentication key: *****
```

Setting the md5 key in ciphertext format:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf message-digest-key 1 md5 ciphertext AQt6e...7qEa4=
```

Deleting the md5 key:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf message-digest-key 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf network

```
ip ospf network {broadcast | point-to-point}
no ip ospf network
```

Description

Configures the OSPF network type for the interface. Choose one of the following parameters as the interface network type.

The **no** form of this command sets the network type for the interface to the system default which is broadcast network.



For an IP unnumbered interface, the network type should be configured as a **point-to-point**.

Parameter	Description
broadcast	Specifies the OSPF network type as a broadcast multi-access network.
point-to-point	Specifies the OSPF network type as a point-to-point network.

Examples

Setting OSPF network type for the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf network broadcast
switch(config-if-vlan)# ip ospf network point-to-point
```

Disabling OSPF network type for the interface to system default of broadcast network:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf network
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf passive

```
ip ospf passive
no ip ospf passive
```

Description

Configures the interface as an OSPF passive interface. With this setting, the interface participates in OSPF but does not send or receive packets on that interface.

The **no** form of this command resets the interface as active. With this setting, the interface starts sending and receiving OSPF packets.

Examples

Setting the interface as OSPF passive interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf passive
```

Setting the interface as OSPF active interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf passive
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf priority

```
ip ospf priority <PRIORITY-VALUE>
no ip ospf priority
```

Description

Sets the OSPF priority for the interface. The larger the numeric value of the priority, the higher the chances for it to become the designated router. Setting a priority of zero makes the router ineligible to become a designated router or back up designated router.

The **no** form of this command sets the OSPF priority for the interface to the default of 1.

Parameter	Description
<PRIORITY-VALUE>	Specifies the OSPF priority value. Range: 0 to 255. Default: 1.

Examples

Setting OSPF priority for the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf priority 50
```

Disabling OSPF priority for the interface to default:

```
switch(config)# interface vlan1
switch(config-if-vlan)# no ip ospf priority
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf retransmit-interval

```
ip ospf retransmit-interval <INTERVAL>
no ip ospf retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for the OSPF interface.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default of 5 seconds for the OSPF interface.

Parameter	Description
<INTERVAL>	Specifies the retransmit interval, in seconds. Range: 1 to 3600. Default: 5.

Examples

Setting OSPF retransmit interval on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf retransmit-interval 30
```

Setting OSPF retransmit interval to the default on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf retransmit-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	

ip ospf sha-key sha

```
ip ospf sha-key <KEY-ID> sha [{ciphertext | plaintext} <KEY>]
no ip ospf sha-key <KEY-ID>
```

Description

Sets the SHA (secure hash authentication) key for the selected interface. If the SHA key is given in ciphertext, it will be decrypted and applied to the protocol. This command accepts a key of up to 64 characters irrespective of the SHA version configured on the interface. OSPF will internally pad zeros to the key to obtain a 64-byte key. For all types of SHA, key length is adjusted to 64 bytes.

The **no** form of this command deletes the SHA authentication key.

Parameter	Description
<KEY-ID>	Specifies the SHA key ID. Range: 1 to 255.
{ciphertext plaintext}	Selects the SHA key format.
<KEY>	Specifies the SHA authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting the SHA authentication key in plaintext format:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf sha-key 1 sha plaintext F82#450b
```

Setting the SHA authentication key in prompted plaintext format:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf sha-key 1 sha
Enter the SHA authentication key: *****
Re-Enter the SHA authentication key: *****
```

Setting the SHA authentication key in ciphertext format:

```
switch(config)# interface 1/1/1
switch(config-if)# ip ospf sha-key 1 sha ciphertext AQapu...C2K47A=
```

Deleting the SHA authentication key:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip ospf sha-key 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip ospf shutdown

```
ip ospf shutdown
no ip ospf shutdown
```

Description

Disables OSPF on the interface. The interface state changes to Down. It does not remove the interface from the OSPF area. To remove the interface, use the command **no ip ospf area**.

The **no** form of this command re-enables OSPF on the interface

Examples

Disabling OSPF on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf shutdown
```

Re-enabling OSPF on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf shutdown
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip ospf transit-delay

```
ip ospf transit-delay <DELAY>
no ip ospf transit-delay
```

Description

Sets the time delay in link state transmission for the OSPF interface.

The **no** form of this command sets the delay in link state transmission to the default of 1 second for the OSPF interface.

Parameter	Description
<DELAY>	Specifies the transit delay in seconds. Range: 1 to 3600. Default: 1.

Examples

Setting OSPF transit delay on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ip ospf transit-delay 30
```

Setting OSPF transit delay to the default on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ip ospf transit-delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

keychain

```
keychain <KEYCHAIN-NAME>
no keychain
```

Description

Sets the key chain for md5 authentication. A key chain configures rotating keys for packet authenticating, reducing the risk of keys being compromised.

The **no** form of this command deletes the key chain used for md5 authentication.

Parameter	Description
<KEYCHAIN-NAME>	Name of key chain to be used for md5 authentication.

Examples

Setting OSPF virtual link key chain authentication:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# keychain ospf_keys
```

Deleting OSPF virtual link key chain authentication:

```
switch# configure terminal
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# no keychain
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

max-metric router-lsa

```
max-metric router-lsa [on-startup [<ADVERT-TIME>]]
no max-metric router-lsa [on-startup]
```

Description

Sets the protocol to advertise a maximum metric so that other routers do not prefer this router as an intermediate hop in their shortest path first (SPF) calculations. If the on-startup parameter is used, the router is configured to advertise a maximum metric at startup for the time mentioned in seconds or for a default value of 600 seconds.

The **no** form of this command advertises the normal cost metrics instead of advertising the maximized cost metric. This setting causes the router to be considered in traffic forwarding.

Parameter	Description
<code>on-startup <ADVERT-TIME></code>	Specifies the time in seconds to advertise self as stub-router on startup. If no time is specified, the default time of 600 seconds is used. Range: 5 to 86400. Default: 600.

Examples

Setting to maximize the cost metrics for Router LSA:

```
switch(config)# router ospf 1
switch(config-ospf-1)# max-metric router-lsa
switch(config-ospf-1)# max-metric router-lsa on-startup
switch(config-ospf-1)# max-metric router-lsa on-startup 3000
```

Setting to advertise the normal cost metrics instead of advertising the maximized cost metric:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no max-metric router-lsa
switch(config-ospf-1)# no max-metric router-lsa on-startup
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospf-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

maximum-paths

```
maximum-paths <MAX-VALUE>
no maximum-paths
```

Description

Sets the maximum number of ECMP routes that OSPF can support.

The **no** form of this command sets the maximum number of ECMP routes that OSPF can support to the default value of 4.

Parameter	Description
<code><MAX-VALUE></code>	Specifies the maximum number of ECMP routes. Range: 1 to 32. Default: 4.

Examples

Setting maximum number of ECMP routes:

```
switch(config)# router ospf 1
switch(config-ospf-1)# maximum-paths 32
```

Setting maximum number of ECMP routes to the default of 4:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no maximum-paths
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10	Increased upper limit of range of <MAX-VALUE> parameter to 32.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospf-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

message-digest-key md5

```
message-digest-key <KEY-ID> md5 [{ciphertext | plaintext} <KEY>]
no message-digest-key <KEY-ID>
```

Description

Sets the virtual link md5 message digest authentication key. If the md5 key is given in ciphertext, it will be decrypted and applied to the protocol.

The **no** form of this command deletes the virtual link md5 authentication key.

Parameter	Description
<KEY-ID>	Specifies the virtual link md5 key ID. Range: 1 to 255.
{ciphertext plaintext}	Selects the virtual link md5 key format.
<KEY>	Specifies the virtual link md5 authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting virtual link md5 authentication key in plaintext format:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# message-digest-key 1 md5 plaintext F82#450b
```

Setting the virtual link md5 authentication key in prompted plaintext format:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# message-digest-key 1 md5
Enter the MD5 authentication key: *****
Re-Enter the MD5 authentication key: *****
```

Setting the virtual link md5 authentication key in ciphertext format:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# message-digest-key 1 md5 ciphertext AQapu...C2K47A=
```

Deleting the virtual link md5 authentication password:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# no message-digest-key 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

passive-interface default

```
passive-interface default
no passive-interface
```

Description

Configures all OSPF interfaces as passive.

The **no** form of this command sets all OSPF interfaces as active.

Examples

Setting OSPF-enabled interfaces as passive:

```
switch(config)# router ospf 1
switch(config-ospf-1)# passive-interface default
```

Setting OSPF-enabled interfaces as active:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no passive-interface
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute {bgp | connected | host-routes | local loopback | static | rip | ospf
<PROCESS-ID>[route-map <ROUTE-MAP-NAME>]}
no redistribute {bgp | connected | host-routes | local loopback | static | rip | ospf
<PROCESS-ID>}[route-map <ROUTE-MAP-NAME>]}
```

Description

Redistributes routes originating from other protocols, or from another OSPFv2 process, to the current OSPFv2 process.

If a route map is specified, then only the routes that pass the match clause specified in the route map are redistributed to OSPFv2. Configuration is not allowed if the referenced route map has not yet been configured.

If you try to redistribute routes from an OSPFv2 process which is not created, you are prompted to allow the OSPFv2 process to be auto-created before proceeding with redistribution. If you confirm at the prompt, the OSPFv2 process is created with defaults and redistribution configuration applied. If you deny at the prompt, redistribution configuration is skipped.

If command **route-redistribute active-routes-only** has been issued, only the routes from other protocols which are selected for forwarding are considered for redistribution into OSPFv2.

The **no** form of this command disables redistribution of routes to the current OSPFv2 process.

Parameter	Description
bgp	Specifies redistributing BGP (Border Gateway Protocol) routes.
connected	Specifies redistributing connected (directly attached subnet or host).
host-routes	Redistributes ARP entries. ARP entries learnt through EVPN or over VXLAN tunnels are not redistributed. The host-routes parameter is applicable to HPE Aruba Networking 8325, 10000, 8360, and 9300/9300S Switch series only.
local loopback	Specifies redistributing local routes of the loopback interface.
static	Specifies redistributing static routes.
rip	Specifies redistributing RIP routes.
ospf <PROCESS-ID>	Specifies redistributing routes from the specified OSPFv2 process ID. Range: 1 to 65535.
route-map <ROUTE-MAP-NAME>	Specifies redistribution filtering by route map. To create a route map, use command route-map .

Examples

Redistributing routes to OSPFv2:

```
switch(config)# router ospf 1
switch(config-ospf-1)# redistribute bgp
switch(config-ospf-1)# redistribute bgp route-map BGP_routes
```

```
switch(config-ospf-1)# redistribute host-routes
switch(config-ospf-1)# redistribute connected
switch(config-ospf-1)# redistribute connected route-map connected_routes
switch(config-ospf-1)# redistribute local loopback
switch(config-ospf-1)# redistribute local loopback route-map local_routes
switch(config-ospf-1)# redistribute static
switch(config-ospf-1)# redistribute static route-map static_networks
switch(config-ospf-1)# redistribute rip
switch(config-ospf-1)# redistribute rip route-map rip-routes
```

```
switch(config-ospf-1)# redistribute ospf 2
```

Disabling redistributing routes to OSPFv2:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no redistribute bgp
switch(config-ospf-1)# no redistribute bgp route-map BGP_routes
```

```
switch(config-ospf-1)# no redistribute host-routes
switch(config-ospf-1)# no redistribute connected
switch(config-ospf-1)# no redistribute connected route-map connected_routes
switch(config-ospf-1)# no redistribute local loopback
switch(config-ospf-1)# no redistribute local loopback route-map local_routes
switch(config-ospf-1)# no redistribute static
switch(config-ospf-1)# no redistribute static route-map static_networks
switch(config-ospf-1)# no redistribute rip
switch(config-ospf-1)# no redistribute rip route-map rip-routes
switch(config-ospf-1)# no redistribute ospf 2
```

Redistributing ARP entries:

```
switch(config-ospf-1)# redistribute host-routes route-map host_routes12
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.13	Added route-map support for host-routes .
10.12	Added information about the host-routes parameter.
10.08	Added route-map support for supported redistribute source-protocols. Updated information and examples.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

reference-bandwidth

```
reference-bandwidth <BANDWIDTH>
no reference-bandwidth
```


Description

Sets the reference bandwidth for OSPFv2. If the OSPFv2 interface cost is not explicitly set, then the cost of all the OSPFv2 interfaces is recalculated based on the reference bandwidth and link speed of the interface.

For VLAN interfaces the link speed value is taken as 1 Gbps (if the OSPFv2 interface cost is not explicitly set).

The **no** form of this command sets the reference bandwidth for OSPF to the default of 100000 Mbps.

Parameter	Description
<code><BANDWIDTH></code>	Specifies the reference bandwidth used to calculate the cost of an interface in Mbps. Range: 1 to 4000000. Default: 100000.

Examples

Setting the reference bandwidth:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# reference-bandwidth 40000
```

Setting the reference bandwidth to the default value:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# no reference-bandwidth
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf- <code><PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

retransmit-interval

```
retransmit-interval <INTERVAL>  
no retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for virtual links.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default of 5 seconds for virtual links.

Parameter	Description
<INTERVAL>	Specifies the retransmit interval in seconds. Range: 1 to 3600. Default: 5.

Examples

Setting OSPFv2 virtual links retransmit interval:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# retransmit-interval 30
```

Setting OSPFv2 virtual links retransmit interval to default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# no retransmit-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

rfc1583-compatibility

```
rfc1583-compatibility
no rfc1583-compatibility
```

Description

Enables OSPF compatibility with RFC1583 (backward compatibility). If RFC1583 compatibility is enabled, then the route cost calculation follows a different method.

The **no** form of this command disables OSPF compatibility with RFC1583 (backward compatibility). By default the RFC1583 compatibility is disabled.

Examples

Enabling OSPF RFC1583 compatibility:

```
switch(config)# router ospf 1
switch(config-ospf-1)# rfc1583-compatibility
```

Disabling OSPF RFC1583 compatibility:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no rfc1583-compatibility
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

router ospf

```
router ospf <PROCESS-ID> [vrf <VRF-NAME>]
no router ospf <PROCESS-ID> [vrf <VRF-NAME>]
```

Description

Creates an OSPF process (if not created already) on a VRF, and switches to the OSPF router instance context. Up to eight OSPF processes are supported per VRF.

The **no** form of this command removes the OSPF instance.

Parameter	Description
<PROCESS-ID>	Specifies an OSPF process ID. Range: 1 to 65535.
vrf <VRF-NAME>	Specifies a VRF name for the OSPF process. Default: default.

Examples

```
switch(config)# router ospf 1
switch(config-ospf-1)#
```

```
switch(config)# router ospf 1 vrf vrf_red
```

```
switch(config)# no router ospf 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

router-id

```
router-id <ROUTER-ADDR>  
no router-id
```

Description

Sets an ID for the router in an IPv4 address format.

The **no** form of this command unconfigures the router-id for the instance and sets the router-id to the default as follows: the router-id is selected dynamically as equal to the highest loopback address on the router, or the highest active interface if there are no loopback addresses. If no IP address is configured on any interfaces on the router, OSPF will not form an adjacency.

Parameter	Description
<ROUTER-ADDR>	Specifies the Router ID in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Setting router-id in the OSPF context:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# router-id 1.1.1.1
```

Unconfiguring router-id:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# no router-id
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

sha-key sha

```
sha-key <KEY-ID> sha [{ciphertext | plaintext}] <KEY>]
no sha-key <KEY-ID>
```

Description

Sets the SHA (secure hash authentication) key for the selected virtual link. If the SHA key is given in ciphertext, it will be decrypted and applied to the protocol. This command accepts a key of up to 64 characters irrespective of the SHA version configured on virtual link. OSPF will internally pad zeros to the key to obtain a 64-byte key. For all types of SHA, key length is adjusted to 64 bytes.

The **no** form of this command deletes the virtual link SHA authentication key.

Parameter	Description
<KEY-ID>	Specifies the virtual link SHA key ID. Range: 1 to 255.
{ciphertext plaintext}	Selects the virtual link SHA key format.
<KEY>	Specifies the virtual link SHA authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting virtual link SHA authentication key in plaintext format:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# sha-key 1 sha plaintext F82#450b
```

Setting the virtual link SHA authentication key in prompted plaintext format:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# sha-key 1 sha
Enter the SHA authentication key: *****
Re-Enter the SHA authentication key: *****
```

Setting the virtual link SHA authentication key in ciphertext format:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# sha-key 1 sha ciphertext AQapu...C2K47A=
```

Deleting the virtual link SHA authentication key:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink)# no sha-key 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

show ip ospf

```
show ip ospf [<PROCESS-ID>] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays general OSPF, area, state, and configuration information.

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display general OSPF information for a particular OSPF process. Range: 1 to 65535.
all-vrfs	Optionally select to display general OSPF information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing general OSPF configurations:

```
switch# show ip ospf 200
VRF : Default                                Process : 200
-----

Router ID          : 1.1.1.1                OSPFv2           : Enabled
BFD                : Disabled               SPF Start Interval : 5000 ms
SPF Hold Interval  : 1000 ms                SPF Max Wait Interval : 1000 ms
LSA Start Interval : 5000 ms                LSA Hold Interval   : 1000 ms
LSA Max Wait Interval : 1000 ms             LSA Arrival Interval : 1000 ms
External LSAs      : 4                     Checksum Sum        : 133302
ECMP               : 4                     Reference Bandwidth  : 100000 Mbps
Area Border        : Yes                   AS Border          : No
GR Status          : Disabled              GR Interval         : 120 sec
GR State           : Inactive              GR Exit Status      : None
GR Helper          : Enabled               GR Strict LSA Check  : Enabled
GR Ignore Lost I/F : Disabled              Internal Process ID  : 1

Summary address:
  prefix 10.1.1.0/24, advertise, tag 10

Area      Total    Active
-----
Normal    2        1
Stub      2        1
NSSA      0        0

Area : 0.0.0.1
-----
Area Type          : Normal      Status           : Active
Total Interfaces   : 100         Active Interfaces : 10
Passive Interfaces : 5           Loopback Interfaces : 85
SPF Calculation Count : 1500

Area ranges:
  ip-prefix 10.1.1.1/24, inter-area, advertise
Number of LSAs      : 5000      Checksum Sum      : 99122
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf border-routers

```
show ip ospf [<PROCESS-ID>]
    border-routers [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays the OSPF routing table entries for Area Border Router (ABR) and Autonomous System Border Router (ASBR).

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display general OSPF information for a particular OSPF process. Range: 1 to 65535.
all-vrfs	Optionally select to display general OSPF information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPF border routers information:

```
switch# show ip ospf border-routers
VRF : default          Process : 1
Internal Routing Table
-----

Codes: i - Intra-area route, I - Inter-area route

  Router-ID    Cost Type Area      SPF  Nexthop  Interface
i 40.40.40.40  10  ABR  0.0.0.0  71    192.0.2.1 1/1/1
i 60.60.60.60  20  ABR  0.0.0.0  71    192.0.2.1 1/1/1
i 40.40.40.40  10  ABR  0.0.0.1  71    192.0.2.1 1/1/2
i 60.60.60.60  20  ABR  0.0.0.1  71    192.0.2.1 1/1/2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf interface


```
show ip ospf [<PROCESS-ID>] interface [<interface-name>] [brief]
[all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Displays general OSPF, area, state, and configuration information.



For an IP unnumbered enabled OSPF interface, the output of the command displays the IP address borrowed from the donor interface.

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display general OSPF information for a particular OSPF process. Range: 1 to 65535.
<interface-name>]	Specify the name of an OSPF interface.
brief	Include this parameter to display a brief overview of the following OSPF configuration information. - Interface: OSPF interface name. - Area: OSPF area ID. - Cost: The metric OSPF uses to judge a path's feasibility, calculated as (reference bandwidth / interface bandwidth). - State: Indicates if the interface is a designated router (Dr) or a backup designated router (Backup-dr). - Status: Indicates if the interface is up or down. - Flags: P - Passive A - Active.
all-vrfs	Optionally select to display general OSPF information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing general OSPF configuration settings for the default VRF:

```
switch (config-if)# show ip ospf 1
VRF : default                               Process : 1
-----

RouterID           : 20.0.0.1                OSPFv2           : Enabled
SPF Start Interval : 200 ms
SPF Hold Interval  : 1000 ms
LSA Start Time     : 5000 ms
LSA Max Wait Time  : 0 ms
External LSAs      : 0
ECMP               : 4
Area Border        : false
GR Status          : Enabled
GR State           : inactive
GR Helper          : Enabled
SPF Max Wait Interval : 5000 ms
LSA Hold Time      : 0 ms
LSA Arrival        : 1000 ms
Checksum Sum       : 0
Reference Bandwidth : 100000 Mbps
AS Border          : false
GR Interval        : 120 sec
GR Exit Status     : none
GR Strict LSA Check : Enabled
```

```
GR Ignore Lost I/F      : Disabled
Summary address:
```

Area	Total	Active
Normal	1	1
Stub	0	0
NSSA	0	0

```
Area : 0.0.0.0
```

Area Type	: Normal	Status	: Active
Total Interfaces	: 1	Active Interfaces	: 1
Passive Interfaces	: 0	Loopback Interfaces	: 0
SPF Calculation Count	: 4		
Area ranges	:		
Number of LSAs	: 3	Checksum Sum	: 82420

Showing OSPF configuration settings for all interfaces:

```
switch(config)# show ip ospf interface
```

```
Codes: DR - Designated router BDR - Backup designated router
```

```
Interface 1/1/1 is up, line protocol is up
```

VRF	: default	Process	: 1
IP Address	: 10.10.10.1/24	Area	: 0.0.0.0
Status	: Up	Network Type	: Broadcast
Hello Interval	: 10 sec	Dead Interval	: 40 sec
Transit Delay	: 1 sec	Retransmit Interval	: 5 sec
Link Speed	: 1000 Mbps		
Cost Configured	: 1	Cost Calculated	: 1
State/Type	: BDR	Router Priority	: 1
DR	: 10.10.10.2	BDR	: 10.10.10.1
Link LSAs	: 0	Checksum Sum	: 0
Authentication	: Md5	Passive	: Yes

```
Interface 1/1/2 is up, line protocol is up
```

VRF	: default	Process	: 1
IP Address	: 10.10.10.1/24	Area	: 0.0.0.0
Status	: Up	Network Type	: Broadcast
Hello Interval	: 10 sec	Dead Interval	: 40 sec
Transit Delay	: 1 sec	Retransmit Interval	: 5 sec
Link Speed	: 1000 Mbps		
Cost Configured	: 1	Cost Calculated	: 1
State/Type	: BDR	Router Priority	: 1
DR	: 20.10.10.2	BDR	: 20.10.10.1
Link LSAs	: 0	Checksum Sum	: 0
Authentication	: Simple	Passive	: No

Displaying brief OSPF information

```
switch(config-if)# show ip ospf interface brief
```

```
VRF : default Process : 1
```

```
=====
```

```
Total Number of Interfaces: 2
```

```
Flags: P - Passive A - Active
```

Interface	Area	IP Address/Mask	Cost	State	Status	Flags

```

-----
-----
1/1/1      0.0.0.0      10.10.10.1/24      40      DR      Up      P
1/1/2      255.255.255.255  200.200.200.123/24  4      Waiting Up      A

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14.1000	, The output of the command displays the borrowed IP address for an IP unnumbered enabled OSPF interface.
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.09	Output of the show ip ospf interface command includes flags to indicate whether the interface is in passive or active mode.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf lsdb

```

show ip ospf [<process-id>] lsdb
  adv-router {<ROUTER-ID> | self}
  area <AREA-ID>
  lsid <link-state-id>
  all-vrfs [{vrf <VRF-NAME>}]
  asbr-summary
  database-summary
  external
  lsid <LINK-STATE-ID>
  network
  nssa-external
  router
  summary

```

Description

Shows the OSPF link state database summary for different OSPF LSAs (Link State Advertisement). Use the parameters to get information for a particular LSA.

Parameter	Description
<code><PROCESS-ID></code>	Enter an OSPF process ID to display general OSPF information for a particular OSPF process. Range: 1 to 65535.
<code>adv-router {<ROUTER-ID> self}</code>	Select to display link states for a particular advertising router. Specify either a Router ID of the advertising router or specify self to show self-originated link states.
<code>area <AREA-ID></code>	Select to display information filtered for the specified area in one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Value: 0 to 4294967295.
<code>lsid <LINK-STATE-ID></code>	Select to display information filtered by link state identifier specified in IPv4 address format (A.B.C.D).
<code>all-vrfs {vrf <vrf-name>}</code>	Select all-vrfs to display general OSPF information for all VRFs, or use the vrf <VRF-NAME> option to display information for a specific VRF. Optionally select one of the following parameters to filter the link state database information.
<code>asbr-summary</code>	Show ASBR summary link states (LSA type 4).
<code>database-summary</code>	Select to display the count of each type of LSA and each area in the database. NOTE: The database-summary parameter does not support the area <area-id> , lsid <link-state-id> or adv-router {<router-id> self} parameters.
<code>external</code>	Show external link states (LSA type 5). NOTE: The external parameter does not support the area <area-id> parameter.
<code>network</code>	Show network LSAs (LSA type 2).
<code>nssa-external</code>	Show NSSA external link states (LSA type 7).
<code>router</code>	Show router LSAs (LSA type 1).
<code>summary</code>	Show network-summary link states (LSA type 3).

Examples

Showing OSPF link state database (LSDB) general information:

```
switch# show ip ospf lsdb
OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
```

```

-----
ADV Router      Age      Seq#      Checksum    LSID      Link Count  Bits
-----
40.40.40.40    930     0x80000004 0x2ea1     0         3          None
50.50.50.50    935     0x80000002 0x8b52     0         1          E
60.60.60.60    943     0x800003c5 0x9854     0         2          None

Network Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Router Count
-----
60.60.60.60    944     0x80000001 0x7179     1360007168 2
50.50.50.50    935     0x80000001 0x516a     19         1

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40    929     0x80000001 0x2498     131072     FEC0:3344::/32
50.50.50.50    928     0x80000001 0x5b2f     65536      111::/64

Inter Area Router Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Destination Router ID
-----
40.40.40.40    929     0x80000001 0x2498     1          33.33.33.33

AS External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40    264     0x80000001 0x24cc4     1          10::/64
40.40.40.40    675     0x80000001 0x5b00f     2          11::/64

NSSA External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
3.3.3.3        264     0x80000001 0x24ac2     1          200::/64

Link-local Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Interface
-----
50.50.50.50    264     0x80000001 0x653c4     19         1/1/1

Intra Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
-----
ADV Router      Age      Seq#      Checksum    LSID      Referenced LS Type
Referenced LSID
-----
50.50.50.50    263     0x80000001 0x1da34     1          0x2001          0
50.50.50.50    264     0x80000001 0x2a45d     1          0x2002          19

```

Showing ASBR summary link states:

```

switch# show ip ospf lsdbr asbr-summary
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

```

ASBR Summary Link State Advertisements (Area 0.0.0.0)

LSID	ADV Router	Age	Seq#	Checksum
209.165.201.3	60.60.60.60	944	0x80000001	0x7179
192.0.2.1	50.50.50.50	935	0x80000001	0x516a

Showing external link states:

```
switch# show ip ospf lsdb external
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====
```

AS External Link State Advertisements

LSID	ADV Router	Age	Seq#	Checksum
209.165.201.3	60.60.60.60	944	0x80000001	0x7179
192.0.2.1	50.50.50.50	935	0x80000001	0x516a

Showing database summary:

```
switch# show ip ospf lsdb database-summary
OSPF Router with ID (10.1.1.1) (Process ID 1 VRF default)
=====
```

Area 0.0.0.0 database summary

LSA Type	Count
Router	2
Network	1
Inter-area Summary	1
ASBR Summary	0
NSSA External	0
Subtotal	4

Process 1 database summary

LSA Type	Count
Router	2
Network	1
Inter-area Summary	1
ASBR Summary	0
NSSA External	0
AS External	0
Total	4

Showing router LSAs:

```
switch# show ip ospf lsdb router
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
-----
```

LSID	ADV Router	Age	Seq#	Checksum	Link Count
1.1.1.2	1.1.1.2	15	0x80000004	0xf526	1
2.2.2.1	2.2.2.1	14	0x80000005	0x6c5e	2
2.2.2.2	2.2.2.2	104	0x80000004	0xf51a	1

```
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
-----
```

LSID	ADV Router	Age	Seq#	Checksum	Link Count
1.1.1.2	1.1.1.2	15	0x80000004	0xf526	1
2.2.2.1	2.2.2.1	14	0x80000005	0x6c5e	2
2.2.2.2	2.2.2.2	104	0x80000004	0xf51a	1

Showing network LSAs:

```
switch# show ip ospf lsdb network
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

Network Link State Advertisements (Area 0.0.0.0)
-----
```

LSID	ADV Router	Age	Seq#	Checksum
1.1.1.2	1.1.1.2	141	0x80000001	0xc55e
2.2.2.2	2.2.2.2	230	0x80000001	0xa179

Showing network-summary link states:

```
switch# show ip ospf lsdb summary
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

Inter-area Summary Link State Advertisements (Area 0.0.0.0)
-----
```

LSID	ADV Router	Age	Seq#	Checksum
1.1.1.0	2.2.2.1	133	0x80000002	0xa089

```
Inter-area Summary Link State Advertisements (Area 0.0.0.1)
-----
```

LSID	ADV Router	Age	Seq#	Checksum
2.2.2.0	2.2.2.1	133	0x80000002	0x7caa

Showing NSSA external link states:

```

switch(config-ospf-1)# show ip ospf lsdb nssa-external
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

NSSA External Link State Advertisements (Area 0.0.0.1)
-----

LSID                ADV Router    Age      Seq#          Checksum
-----
8.8.8.0             1.1.1.2      162     0x80000003   0xc7b2

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf neighbors

```

show ip ospf [<PROCESS-ID>] neighbors [<NEIGHBOR-ID>]
    [interface <INTERFACE-NAME>] [detail | summary]
    [all-vrfs | vrf <VRF-NAME>]

```

Description

Displays information about OSPF neighbors.

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display OSPF neighbor information for the particular OSPF process. Range: 1 to 65535.
neighbors <NEIGHBOR-ID>	Select to display information about a particular neighbor, specified in IPv4 format (A.B.C.D).
interface <INTERFACE-NAME>	Select to display neighbor information only for the specified interface.
detail	Select to display detailed information for all the neighbors.
summary	Select to display summary information for the neighbors.

Parameter	Description
all-vrfs	Select to display neighbor information for all VRFs.
vrf <VRF-NAME>	Specify the name of a VRF. Default: default.

Examples

Showing OSPF neighbors information for the default VRF:

```
switch# show ip ospf neighbors
OSPF Process ID 1 VRF default
=====

Total Number of Neighbors: 1

Neighbor ID      Priority   State             Nbr Address       Interface
-----
2.2.2.2          1         FULL/DR           10.1.1.2           1/1/1
```



The **Nbr Address** displays the borrowed IP address for IP unnumbered interfaces.

Showing OSPF neighbors information for VRF red:

```
switch# show ip ospf neighbors vrf red
OSPF Process ID 1 VRF red
=====

Total Number of Neighbors: 1

Neighbor ID      Priority   State             Nbr Address       Interface
-----
1.1.1.1          1         FULL/BDR          10.1.1.1           1/1/1
```

Showing OSPF neighbors information for a specific neighbor:

```
switch# show ip ospf neighbors 2.2.2.2
switch# show ip ospf neighbors 2.2.2.2
VRF : default                               Process : 1
-----
Router-Id       : 2.2.2.2                     Area Id         : 0.0.0.0
Interface       : 1/1/1                     Address         : 10.10.10.2
State           : FULL                       Neighbor Priority : 1
Dead Timer Due  : 00:00:36                   Options         : 0x42
```

Showing OSPF neighbors information for a specific neighbor and interface:

```
switch# show ip ospf neighbors 2.2.2.2 interface 1/1/1
VRF : default                               Process : 1
-----
Router-Id       : 2.2.2.2                     Area Id         : 0.0.0.0
Interface       : 1/1/1                     Address         : 10.10.10.2
```

```
State           : FULL                      Neighbor Priority : 1
Dead Timer Due  : 00:00:36                  Options          : 0x42
```

Showing detail information for OSPF neighbors:

```
switch# show ip ospf neighbors detail
VRF : default                      Process : 1
-----

Router-Id       : 2.2.2.2           Area Id         : 0.0.0.0
Interface       : 1/1/1             Address         : 10.10.10.2
State           : FULL              Neighbor Priority : 1
DR              : 10.10.10.2        BDR            : 10.10.10.1
Dead Timer Due  : 00:00:38          Options        : 0x42
Retransmission Queue Length : 0
Time Since Last State Change : 00h:11m:37s
```

Showing summary information for OSPF neighbors in the **default** VRF:

```
switch# show ip ospf neighbors summary
OSPF Process ID 1 VRF default, Neighbor Summary
=====

Interface  Down  Attempt  Init  TwoWay  ExStart  Exchange  Loading  Full  Total
-----
1/1/1      0    0        0    0       0        0        0        1    1
1/1/2      0    0        0    0       0        0        0        0    0
Total      0    0        0    0       0        0        0        1    1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14.1000	The output parameter, Nbr Address displays the borrowed IP address for IP unnumbered interfaces.
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf routes

```
show ip ospf [<PROCESS-ID>] routes
    [<IPv4-ADDR>/<MASK>] protected [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays OSPF routing information.

Parameter	Description
<IPv4-ADDR>	Specify an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.
<PROCESS-ID>	Enter an OSPF process ID to display OSPF neighbor information for the particular OSPF process. Range: 1 to 65535.
all-vrfs	Select to display neighbor information for all VRFs.
vrf <VRF-NAME>	Specify the name of a VRF. Default: default.
protected	Selects a protected route. Specifying an IPv4 address will select protected route for that prefix.

Examples

Showing OSPF routing table information:

```
switch# show ip ospf routes
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table
-----

Total Number of Routes : 2

10.1.1.0/24          (i) area: 0.0.0.0
    directly attached to interface 1/1/1, cost 1 distance 110
20.1.1.0/24          (I)
    via 10.1.1.2 interface 1/1/1, cost 2 distance 110
```

Showing OSPF routing table information for a specific subnet:

```
switch# show ip ospf routes 10.1.1.0/2
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1 VRF default, Routing Table for prefixes 10.1.1.0/24
-----

Total Number of Routes : 1

10.1.1.0/24          (i) area: 0.0.0.0
    directly attached to interface 1/1/1, cost 1 distance 110
```

Showing OSPF routing table information for a specific protected subnet on the default VRF:

```

switch# show ip ospf routes 211.0.0.0/24 protected vrf default
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes for prefixes 211.0.0.0/24
-----

211.0.0.0/24      (i) area: 0.0.0.0
                  via 110.110.110.1, interface vlan20, cost 122
                  bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 1

```

Showing OSPF routing table information for a specific protected subnet on all VRFs

```

switch# show ip ospf routes 211.0.0.0/24 protected all-vrfs
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes for prefixes 211.0.0.0/24
-----

211.0.0.0/24      (i) area: 0.0.0.0
                  via 110.110.110.1, interface vlan20, cost 122
                  bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 1

```

Showing OSPF routing table information for a specific protected subnet:

```

switch# show ip ospf routes 211.0.0.0/24 protected
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes for prefixes 211.0.0.0/24
-----

211.0.0.0/24      (i) area: 0.0.0.0
                  via 110.110.110.1, interface vlan20, cost 122
                  bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 1

```

Showing OSPF routing table information for all protected routes:

```

switch# show ip ospf routes 211.0.0.0/24 protected
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes
-----

120.120.120.0/24  (i) area: 0.0.0.0
                  via 110.110.110.1, interface vlan20, cost 120
                  bkp 130.130.130.1, interface vlan22, cost 230

```

```

140.140.140.0/24      (i) area: 0.0.0.0
    via 110.110.110.1, interface vlan20, cost 130
    bkp 130.130.130.1, interface vlan22, cost 220

211.0.0.0/24         (i) area: 0.0.0.0
    via 110.110.110.1, interface vlan20, cost 122
    bkp 130.130.130.1, interface vlan22, cost 132

Total Number of Routes : 3

OSPFs Process ID 1, VRF red, Protected Routes
-----

Total Number of Protected Routes: 0

```

Showing OSPF routing table information for protected routes on the default VRF:

```

switch# show ip ospf routes protected vrf default
Codes: i - Intra-area route, I - Inter-area route
      E1 - External type-1, E2 - External type-2

OSPF Process ID 1, VRF default, Protected Routes
-----

140.140.140.0/24      (i) area: 0.0.0.0
    via 130.130.130.1, interface vlan22, cost 130
    bkp 110.110.110.1, interface vlan20, cost 220

211.0.0.0/24         (i) area: 0.0.0.0
    via 110.110.110.1, interface vlan20, cost 122
    bkp 130.130.130.1, interface vlan22, cost 132

120.120.120.0/24      (i) area: 0.0.0.0
    via 110.110.110.1, interface vlan20, cost 120
    bkp 130.130.130.1, interface vlan22, cost 230

Total Number of Routes : 3

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Introduces the protected parameter.
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf statistics

`show ip ospf [<PROCESS-ID>] statistics [all-vrfs | vrf <VRF-NAME>]`

Description

Displays OSPF statistics.

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display OSPF neighbor information for the particular OSPF process. Range: 1 to 65535.
all-vrfs	Select to display OSPF statistics information for all VRFs.
vrf <VRF-NAME>	Specify the name of a VRF. Default: default.

Examples

Showing OSPF statistics:

```
switch# show ip ospf statistics
OSPF Process ID 1 VRF default, Statistics (cleared 1h 16m 24s ago)
-----
Unknown Interface Drops      : 0
Unknown Virtual Interface Drops : 0
Bad Instance ID Drops        : 0
Bad IP Header Length Drops    : 0
Wrong OSPF Version Drops     : 0
Bad Source IP Drops           : 0
Resource Failure Drops        : 0
Bad Header Length Drops       : 0
Total Drops                   : 0
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf statistics interface

```
show ip ospf [<PROCESS-ID>] statistics interface [<INTERFACE-NAME>]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Displays OSPF statistics for the OSPF-enabled interfaces.

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display OSPF-enabled interface statistics information on the specified OSPF process. Range: 1 to 65535.
<INTERFACE-NAME>	Select to display information only for the specified interface.
all-vrfs	Select to display OSPF-enabled interface statistics information for all VRFs.
vrf <VRF-NAME>	Specify the name of a VRF. Default: default.

Examples

Showing OSPF-enabled interfaces information:

```
switch# show ip ospf statistics interface 1/1/1
OSPF Process ID 1 VRF default, interface 1/1/1 statistics (cleared 0h 30m 28s ago)
=====
Tx Hello Packets      : 101          Rx Hello Packets      : 99
Tx Hello Bytes        : 101          Rx Hello Bytes        : 99
Tx DD Packets         : 101          Rx DD Packets         : 99
Tx DD Bytes           : 101          Rx DD Bytes           : 99
Tx LS Request Packets : 101          Rx LS Requests Packets : 99
Tx LS Request Bytes   : 101          Rx LS Request Bytes   : 99
Tx LS Update Packets  : 101          Rx LS Update Packets  : 99
Tx LS Update Bytes    : 101          Rx LS Update Bytes    : 99
Tx LS Ack Packets     : 101          Rx LS Ack Packets     : 99
Tx LS Ack Bytes       : 101          Rx LS Ack Bytes       : 99

Total Number of State Changes : 8
Number of LSAs                : 29
LSA Checksum Sum               : 2345
Total Transmit Failures       : 29
Total OSPF Packets Discarded   : 999

Reason                        Packets Dropped
-----
Invalid type                  19
Invalid length                 9
Invalid checksum               0
```

```

Invalid version                23
Bad or unknown source          67
Area mismatch                  1
Self-originated                19
Duplicate router ID            9
Interface standby              0
Total Hello packets dropped    60
  Network Mask mismatch        10
  Hello interval mismatch      10
  Dead interval mismatch       10
  Options mismatch             10
  MTU mismatch                 10
  Neighbor ignored             10
Authentication errors          12
  Type mismatch                6
  Authentication failures      6
Wrong protocol                 0
Resource failures              0
Bad LSA length                 0
Others                         0

Total LSAs Ignored : 176
Bad Type             : 10
Bad Length           : 56
Invalid Data         : 55
Invalid Checksum     : 55

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip ospf virtual-links

```
show ip ospf [<PROCESS-ID>] virtual-links [brief] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays the current state and parameters of the OSPF virtual links.

Parameter	Description
<PROCESS-ID>	Enter an OSPF process ID to display information on the OSPF virtual links for the particular OSPF process. Range: 1 to 65535.
brief	Select to display brief overview information for the OSPF virtual links.
all-vrfs	Select to display OSPF virtual links information for all VRFs.
vrf <VRF-NAME>	Specify the name of a VRF. Default: default.

Examples

Showing OSPF virtual links information:

```
switch# show ip ospf virtual-links
Virtual link to router 40.40.40.40 is up
-----

VRF                : default                Process                : 21
Transit Area       : 0.0.0.1                Authentication        : No
Hello Interval     : 10                     Dead Interval         : 40
Transit Delay      : 1                     Retransmit Interval   : 5
Number of Link LSAs : 0                     Checksum Sum          : 0
Number of State Shanges : 4
```

Showing brief overview information for OSPF virtual links:

```
switch# show ip ospf virtual-links brief
OSPF Process ID 1 VRF default
=====

Total Number of Virtual Links: 1

Remote Router      Transit Area      Status
-----
2.2.2.2            0.0.0.1            down
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

summary-address

```
summary-address <IPV4-ADDR>/<MASK> [no-advertise | tag <TAG-VALUE>]
no summary-address <prefix/length> [no-advertise | tag <tag-value>]
```

Description

Summarizes the external routes with the matching address and mask. When advertising this route, its metric is set to the lowest cost path from among the routes that were summarized.

The **no** form of this command disables route summarization.



This command only works for an ASBR (Autonomous System Boundary Router).

Parameter	Description
<IPV4-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.
no-advertise	Do not advertise the aggregate route. Suppress routes that match the specified prefix/mask pair.
tag <TAG-VALUE>	Specify the tag for the aggregate route. The summary prefix will be advertised along with the tag value in External LSAs. Range: 0 to 4294967295

Examples

Setting OSPF route summarization:

```
switch(config)# router ospf 1
switch(config-ospf-1)# summary-address 10.1.0.0/16
```

Disabling route summarization:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no summary-address 10.1.0.0/16
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

timers lsa-arrival

```
timers lsa-arrival <DELAY>
no timers lsa-arrival
```

Description

Configures the minimum delay between receiving the same LSA from a peer. The same LSA is an LSA that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner before the delay expires, the LSA is dropped. Generally, the LSA arrival timer should be set to a value less than or equal to the start-time value for the command **timers throttle lsa start** on the neighbor.

The **no** form of this command sets the LSA timers to default values.

Parameter	Description
<DELAY>	Specifies the delay in milliseconds. Range: 0 to 600000. Default: 1000.

Examples

Setting the LSA arrival timer:

```
switch(config)# router ospf 1
switch(config-ospf-1)# timers lsa-arrival 10
```

Setting the LSA arrival timer to default:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no timers lsa-arrival
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

timers throttle lsa

```
timers throttle lsa start-time <START-TIME> hold-time <HOLD-TIME> max-wait-time <WAIT-TIME>
no timers throttle lsa
```

Description

Configures the timers for LSA generation.

The **no** form of this command sets the LSA timers to default values.

Parameter	Description
start-time <START-TIME>	Specifies the initial wait time in milliseconds after which LSAs are generated. When set to 0, the LSAs are generated without any delay. Range: 0 to 600000. Default: 5000.
hold-time <HOLD-TIME>	Specifies the amount of time, in milliseconds, between regeneration of an LSA. The hold time doubles each time the same LSA must be regenerated, until max-wait-time is reached. When set to 0, LSA regeneration time is not increased. Range: 0 to 600000. Default: 0.
max-wait-time <WAIT-TIME>	Specifies the maximum wait time, in milliseconds, for regeneration of the same LSA. When set to 0, LSA regeneration time is not increased. Range: 0 to 600000. Default: 0.

Examples

Setting the LSA timers:

```
switch(config)# router ospf 1
switch(config-ospf-1)# timers throttle lsa start-time 100 hold-time 1000 max-wait-time 10000
```

Setting LSA timers to default values:

```
switch(config)# router ospf 1
switch(config-ospf-1)# no timers throttle lsa
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

timers throttle spf

```
timers throttle spf start-time <START-TIME> hold-time <HOLD-TINME>
max-wait-time <WAIT-TIME>
no timers throttle spf
```

Description

Configures timers for SPF calculation. There are three timers:

- **start-time** Is the initial delay before an SPF calculation is started. Default is 200 milliseconds.
- **hold-time** Is the progressive backoff time to wait before next scheduled SPF calculation. Default is 1000 milliseconds. If a route change event occurs during this period, the value doubles until it reaches the *max-wait-time*.
- **max-wait-time** Is the maximum time to wait before the next scheduled SPF calculation. Default is 5000 milliseconds. This is used to limit the SPF hold timer and also defines the time to be considered for which the OSPF LSDB has to be stable, after which the SPF throttle mechanism is reset.

The **no** form of this command sets all the configured non-default timers to default value.

Parameter	Description
<START-TIME>	Time in milliseconds to set timer for initial SPF delay. Default: 200.
<HOLD-TINME>	Time in milliseconds to set the minimum hold time between two consecutive SPF calculations. Default: 1000.
<WAIT-TIME>	Time in milliseconds to set the maximum wait time between two consecutive SPF calculations. Default: 5000.

Examples

Setting non-default timer values for SPF throttling:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# timers throttling spf start-time 500 hold-time 3000 max-
wait-time 9000
Switch(config-ospfv3-1)# show running-config current-context
router ospfv3 1
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2 nssa no-summary
    area 0.0.0.3 stub
```

Setting default timer values for SPF throttling after configuring non-default values:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no timers throttling spf
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

transit-delay

```
transit-delay <SECONDS>  
no transit-delay
```

Description

Sets the time delay in Link state transmission for virtual links.

The **no** form of this command sets the delay in Link state transmission to the default of 1 second for virtual links.

Parameter	Description
<SECONDS>	Specifies the time delay for the transit delay, in seconds. Default: 1 second. Range: 1-3600.

Examples

Setting OSPFv2 virtual links transit delay:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# transit-delay 30
```

Setting OSPFv2 virtual links transit delay to default:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink)# no transit-delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

trap-enable

trap-enable
no trap-enable

Description

Enables the notification of the events to be sent as traps to the SNMP management stations for OSPF. The **no** form of this command disables the notification of the events to be sent as traps to the SNMP management stations for OSPF.

Examples

Enabling sending notification of events as traps:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# trap-enable
```

Disabling sending notification of events as traps:

```
switch(config)# router ospf 1  
switch(config-ospf-1)# no trap-enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospf-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

active-backbone

```
active-backbone stub-default-route  
no active-backbone stub-default-route
```

Description

This command enables the router to send a default route to stub areas if there is an active loopback link in the backbone area. The configuration is not required if backbone area has neighbors or passive interfaces configured. By default active backbone detection is enabled.

Examples

```
switch(config)# router ospf 1  
switch(config-ospf-1)# active-backbone stub-default-route
```

```
switch(config)# no active-backbone stub-default-route
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10.1000	Command Introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID> config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area

```
area <AREA-ID>  
no area <AREA-ID>
```

Description

Creates a normal area with <AREA-ID> set if not present. If area is present and is not the normal area, this command changes the area type to normal area.

The **no** form of this command deletes the area with the **<AREA-ID>** specified. The area can be of any type (stub, stub no-summary, and default normal area).

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.

Examples

Creating a normal area:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1.1.1.1
```

Deleting an area:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no area 1
switch(config-ospfv3-1)# no area 1.1.1.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area authentication ipsec

```
area <AREA-ID> authentication ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>]
no area <AREA-ID> authentication
```

Description

Configures IPsec AH authentication for the specified area. OSPFv3 interfaces which have IPsec configured at the interface context will not use area level IPsec.

The **no** form of this command removes IPsec AH authentication for the specified area.



IPsec is not supported for 6in6 tunnel interfaces.

Parameter	Description
<code><AREA-ID></code>	Specifies the area ID is one of the following formats: OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
<code>spi <SPI-INDEX></code>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<code><AUTH-TYPE></code>	Specifies the authentication type: md5 or sha1 .
<code><KEY-TYPE></code>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<code><AUTH-KEY></code>	Specifies the authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting area 0 to use IPsec authentication with a provided plaintext authentication key:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 0 authentication ipsec spi 256 sha1 plaintext  
F82#450
```

Setting area 5 to use IPsec authentication with a prompted plaintext authentication key:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 5 authentication ipsec spi 256 sha1  
Enter the IPsec authentication key: *****  
Re-Enter the IPsec authentication key: *****
```

Removing IPsec authentication from area 1:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no area 1 authentication
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area encryption ipsec

```
area <AREA-ID> encryption ipsec spi <SPI-INDEX> <AUTH-TYPE>
    [<KEY-TYPE> <AUTH-KEY> <ENCR-TYPE> [<KEY-TYPE> <ENCR-KEY>]]
no area <AREA-ID> encryption
```

Description

Configures IPsec ESP with the authentication and encryption algorithm types and keys for the specified area. OSPFv3 interfaces with IPsec configured at the interface context will not use area level IPsec ESP configuration.

The **no** form of this command removes IPsec ESP from the specified area.



IPsec is not supported for 6in6 tunnel interfaces.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.
<ENCR-TYPE>	Specifies the encryption type: des , 3des , aes , or null . NOTE: Encryption type aes is considered to be AES128, AES192 or AES256 based on key length.
<ENCR-KEY>	Specifies the encryption key.



When the authentication key is not provided on the command line, plaintext authentication key prompting occurs upon pressing Enter, followed by encryption type prompting, and finally plaintext encryption key prompting. The entered key characters are masked with asterisks.



When the authentication key and encryption type are provided on the command line but the encryption key is not provided, plaintext encryption key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting area 0 to use IPsec ESP with provided authentication and encryption keys:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 0 encryption ipsec spi 256 md5 plaintext F824eva  
des plaintext F82#450b
```

Setting area 5 to use IPsec ESP with prompted authentication and encryption keys:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 5 encryption ipsec spi 256 md5  
Enter the IPsec authentication key: *****  
Re-Enter the IPsec authentication key: *****  
  
Enter the IPsec encryption type (3des/aes/des/null)? des  
  
Enter the IPsec encryption key: *****  
Re-Enter the IPsec encryption key: *****
```

Setting area 2 to use IPsec ESP with provided authentication password and encryption type but a prompted encryption key:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 2 encryption ipsec spi 256 md5 plaintext F82# des  
Enter the IPsec encryption key: *****  
Re-Enter the IPsec encryption key: *****
```

Setting area 0 to use IPsec ESP with provided plaintext authentication key and null encryption:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 0 encryption ipsec spi 256 md5 plaintext axtw null
```

Removing IPsec ESP from area 0:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no area 0 encryption
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area nssa

```
area <AREA-ID> nssa [no-summary]
no area <AREA-ID> nssa [no-summary]
```

Description

Creates the NSSA area (Not So Stubby Area) with **<AREA-ID>** if not present. If area is present and not NSSA area, this command changes the area type to NSSA area. If **no-summary** is used, area type will be NSSA No-Summary.

The **no** form of this command clears the NSSA area type. That is, the configured area will be changed to default normal area. The **no area <AREA-ID> nssa no-summary** command enables sending inter-area routes into NSSA, but will not unset the area as NSSA.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
nssa [no-summary]	Specifies Not So Stubby Area (NSSA) area type. If area is present and not NSSA area, parameter changes the area type to NSSA area. If no-summary is specified, area type will be NSSA No-Summary, which means do not inject inter-area routes into NSSA.

Examples

Creating an NSSA area for OSPFv3:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1 nssa
switch(config-ospfv3-1)# area 1 nssa no-summary
```

Clearing the NSSA area for OSPFv3:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no area 1 nssa
switch(config-ospfv3-1)# no area 1 nssa no-summary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area range

```
area <AREA-ID> range <IP-PREFIX> type {inter-area | nssa} [no-advertise]
no area <AREA-ID> range <IP-PREFIX> type {inter-area | nssa} [no-advertise]
```

Description

Summarizes the routes with the matching address or masks for OSPFv3. This command only works for border routers.

The **no** form of this command unsets the route summarization for the configured IPv4 prefix address on the ABR. When using the **no** form of the command with the **no-advertise** option, enables advertising this range to other areas.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
range <IP-PREFIX>	Specifies summarizing routes matching the area range prefix/mask.
type {inter-area nssa}	Specifies the type this address aggregation applies to as either inter-area range prefix or NSSA range prefix.
no-advertise	Specifies the address range status as DoNotAdvertise (do not advertise this range to other areas).

Examples

Summarizing inter-area or NSSA paths on OSPFv3:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1 range fd00::/64 type inter-area
switch(config-ospfv3-1)# area 1 range fd00::/64 type nssa
```

```
switch(config-ospfv3-1) # area 1 range fd00::/64 type inter-area no-advertise
```

Unsetting summarization on OSPFv3:

```
switch(config) # router ospfv3 1
switch(config-ospfv3-1) # no area 1 range fd00::/64 type inter-area
switch(config-ospfv3-1) # no area 1 range fd00::/64 type nssa
switch(config-ospfv3-1) # no area 1 range fd00::/64 type inter-area no-advertise
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area stub

```
area <AREA-ID> stub [no-summary]
no area <AREA-ID> stub [no-summary]
```

Description

Creates the stub area with **<AREA-ID>** if not present. If area is present and is not the stub area, this command changes the area type to stub area. If **no-summary** is used, area type will be totally stubby area.

The **no** form of this command unsets the area type as stub. The configured area will be changed to the default normal area. The **no area <AREA-ID> stub no-summary** command will start sending Area Border Router (ABR) summary link advertisements into the stub area, but will not unset the stub area.



ABR does not inject the default route in a Totally Stubby Area with loopback in Area 0.0.0.0. As a workaround, configure a passive interface or active neighbors in the backbone area.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to

Parameter	Description
	4294967295.
stub [no-summary]	Specifies stub area type. If area is present and not stub area, this parameter changes the area type to stub area. If no-summary is specified, area type will be totally stubby area, which means do not inject interarea routes into stub.

Examples

Creating a stub area:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1 stub
switch(config-ospfv3-1)# area 1 stub no-summary
```

Unsetting the stub area type:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1) # no area 1 stub
switch(config-ospfv3-1) # no area 1 sub no-summary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area virtual-link

```
area <AREA-ID> virtual-link <ROUTER-ID>
no area <AREA-ID> virtual-link <ROUTER-ID>
```

Description

Creates an OSPF virtual link with remote ABR (if not created already) and enters the vlink context.

The **no** form of this command deletes an OSPF virtual link with the specified router ID of the remote ABR. If no<**ROUTER-ID**> is specified, the **no** form of the command sets the virtual link to the default settings.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
virtual-link <ROUTER-ID>	Configures a virtual link with the specified router ID of the remote ABR.

Examples

Configuring OSPF virtual links:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
```

Deleting OSPF virtual links:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no area 100 virtual-link 100.0.1.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area default-metric

```
area <AREA-ID> default-metric <METRIC>
no area <AREA-ID> default-metric
```

Description

Sets the cost of default-summary LSAs announced to the stub/nssa areas.

The **no** form of this command resets the cost of the default-summary LSAs announced to stub/nssa areas to the default of 1.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
default-metric <METRIC>	Specifies the default metric of default-summary LSAs announced to the stub/nssa areas, to the specified value. Default: 1. Range: 0 to 16777215.

Examples

Setting cost for default LSA summary:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1 default-metric 2
switch(config-ospfv3-1)# area 1.1.1.1 default-metric 2
```

Setting cost for default LSA summary to default:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no area 1 default-metric
switch(config-ospfv3-1)# no area 0.0.0.1 default-metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

authentication ipsec

```
authentication ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>]
no authentication
```

Description

Configures IPsec AH authentication for the selected Vlink.

The **no** form of this command removes IPsec AH authentication for the selected Vlink.

Parameter	Description
<code>spi <SPI-INDEX></code>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<code><AUTH-TYPE></code>	Specifies the authentication type: md5 or sha1 .
<code><KEY-TYPE></code>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<code><AUTH-KEY></code>	Specifies the authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting area 1 to use IPsec AH authentication for Vlink with provided plaintext key:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch (config-router-vlink6)# authentication ipsec spi 256 sha1 plaintext F82#450
```

Setting area 1 to use IPsec AH authentication for Vlink with prompted plaintext key:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch (config-router-vlink6)# authentication ipsec spi 256 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Removing IPsec AH authentication for Vlink on area 1:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# no authentication
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

clear ipv6 ospfv3 neighbors

```
clear ipv6 ospfv3 [<PROCESS-ID>] neighbor [<NEIGHBOR>] [interface [<INTERFACE-NAME>]]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Resets the neighbor and clears the OSPF neighbor information.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv3 process ID to clear the statistics for the particular OSPFv3 process. Range: 1 to 65535.
<NEIGHBOR>	Specifies the router ID of a neighbor.
<INTERFACE-NAME>	Specifies the OSPFv3 statistics to clear for the specified interface.
all-vrfs	Select to clear the OSPFv3 statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv3 neighbor information:

```
switch# clear ipv6 ospfv3 1 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 1 neighbor 3.3.3.3
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 1 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 1 neighbor 3.3.3.3 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 neighbor 5.5.5.5
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ipv6 ospfv3 neighbor 5.5.5.5 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear ipv6 ospfv3 statistics

```
clear ipv6 ospfv3 [<PROCESS-ID>] statistics [interface [<INTERFACE-NAME>]]  
[all-vrfs | vrf <VRF-NAME>]
```

Description

Clears the OSPFv3 event statistics.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv3 process ID to clear the statistics for the particular OSPFv3 process. Range: 1 to 65535.
<INTERFACE-NAME>	Specifies the OSPFv3 statistics to clear for the specified interface.
all-vrfs	Select to clear the OSPFv3 statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv3 event statistics:

```
switch# clear ipv6 ospfv3 statistics  
switch# clear ipv6 ospfv3 statistics interface 1/1/1  
switch# clear ipv6 ospfv3 statistics interface 1/1/1 vrf vrf_red
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

dead-interval

```
dead-interval <INTERVAL>
no dead-interval
```

Description

Sets the interval after which a neighbor is declared dead if no hello packet comes in for virtual links. The **no** form of this command sets the dead interval to default for virtual links. The default value is 40 seconds (generally four times the hello packet interval).

Parameter	Description
<INTERVAL>	Specifies the time interval for the dead interval, in seconds. Range: 1 to 65535. Default: 40.

Examples

Setting OSPFv3 virtual links dead interval:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# dead-interval 30
```

Setting OSPFv3 virtual links dead interval to default:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

default-information originate

```
default-information originate [metric <METRIC-VALUE>]
no default-information originate [metric <METRIC-VALUE>]
```

Description

Configures OSPFv3 to advertise the default route (::/0) to its neighbors if it is present in the routing table. Optionally, the metric value can be set for default route ::/0. The default value is 1.

The **no** form of this command disables advertisement of the default route.

Parameter	Description
<i>metric <METRIC-VALUE></i>	Specifies the OSPF metric value for the default route. Optional. Default: 1.

Examples

Setting advertisement of the default route:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# default-information originate
```

Disabling advertisement of the default route:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no default-information originate
```

Setting advertisement of the default route and specifying an optional metric value of 20:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# default-information originate
switch(config-ospfv3-1)# default-information originate metric 20
```

Disabling advertisement of the default route and setting metric to the default value:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no default-information originate metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Added parameter: metric <METRIC-VALUE>
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

default-metric

```
default-metric <METRIC-VALUE>
no default-metric
```

Description

Sets the default metric for redistributed routes in the OSPFv3.

The **no** form of this command sets the default metric to be used for redistributed routes into OSPFv3 to the default of 25.

Parameter	Description
<METRIC-VALUE>	Specifies the default metric value to use for redistributed routes. Range: 1 to 1677214. Default: 25.

Examples

Setting default metric for redistributed routes:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# default-metric 36
```

Setting default metric for redistributed routes to the default:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no default-metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables the OSPFv3 process. By default OSPFv3 process is enabled.
This command does not remove the OSPFv3 configurations.

Example

Disabling OSPFv3 process:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

distance

```
distance [<DISTANCE-VAL> | intra-area [<DISTANCE-VAL>] | inter-area [<DISTANCE-VAL>] |  
external [<DISTANCE-VAL>]]  
no distance [<DISTANCE-VAL> | intra-area [<DISTANCE-VAL>] | inter-area [<DISTANCE-VAL>] |  
external [<DISTANCE-VAL>]]
```

Description

Defines an administrative distance for OSPFv3. Administrative distance is used as a criteria to select the best route when the same route is learned by multiple routing protocols.

The **no** form of this command sets the OSPFv3 administrative distance to the default value of 110. Optionally, administrative distance can be set to default for the specific OSPF route type: intra-area, inter-area, or external type-5 and type-7 routes.

Parameter	Description
<DISTANCE-VAL>	Specifies the OSPFv3 administrative distance. Range: 1 to 255. Default: 110.
intra-area	Specifies the OSPFv3 distance for intra-area routes.

Parameter	Description
inter-area	Specifies the OSPFv3 distance for inter-area routes.
external	Specifies the OSPFv3 distance for external type 5 and type 7 routes.

Usage

Within a given OSPF process, intra-area routes are always given precedence even when distances are configured for inter-area or external type routes.

Examples

Setting OSPFv3 administrative distance:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# distance 100
switch(config-ospfv3-1)# distance intra-area 24 external 55 inter-area 66
switch(config-ospfv3-1)# distance intra-area 24 external 55
switch(config-ospfv3-1)# distance external 55
switch(config-ospfv3-1)#exit

switch(config)# router ospfv3 2
switch(config-ospfv3-2)# distance 200
switch(config-ospfv3-2)# distance external 60
switch(config-ospfv3-2)# distance intra-area 24 inter-area 66
```

Setting OSPFv3 administrative distance to the default:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no distance
switch(config-ospfv3-1)# no distance external
switch(config-ospfv3-1)# no distance intra-area
switch(config-ospfv3-1)# no distance inter-area
switch(config-ospfv3-1)# no distance 1
switch(config-ospfv3-1)#exit

switch(config)# router ospfv3 2 vrf blue
switch(config-ospfv3-2)# no distance 200
switch(config-ospfv3-2)# no distance external 60
switch(config-ospfv3-2)# no distance intra-area 24 inter-area 66
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Added capability to have individual admin distance for multiple OSPF processes in a VRF.
10.09	Added parameters: intra-area , inter-area , external
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

distribute-list prefix

```
distribute-list prefix <prefix-list-name> {in | out}  
no distribute-list prefix <prefix-list-name> {in | out}
```

Description

This command uses an existing prefix list to filter routes that are being installed in the routing table or redistributed to another routing protocol.

The **distribute-list prefix** command filters routes in the inbound or the outbound direction. When this command is issued with the **in** parameter, it filters routes from being installed in the routing table, it does not filter LSAs. When this command is issued with the **out** parameter, it filters only the desired redistributed routes from other protocols.



This command requires that your prefix list is already defined using the [ipv6 prefix](#) commands. Route-maps are not supported with the distribute-list feature.

Parameter	Description
prefix <prefix-list-name>	Specify the name of an existing prefix.
{in out}	Select one of the following parameters to set the filter direction: ▪ in: Filter incoming routes into the routing table ▪ out: Filter outgoing routing updates

Examples

The following commands enable the filtering of OSPFv3 routes in an IPv6 network, so routes are no longer installed in the routing table or redistributed from another routing protocol.

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# distribute-list prefix listA in  
switch(config-ospfv3-1)# distribute-list prefix listB out
```

The following command disables the filtering of OSPFv3 routes in an IPv6 network, so routes can be installed in the routing table or redistributed from another routing protocol.

```
switch# configure terminal  
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no distribute-list prefix listA in  
switch(config-ospfv3-1)# no distribute-list prefix listB out
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables OSPFv3 process when disabled. By default OSPFv3 process is enabled.

Example

Enabling OSPFv3 process:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

encryption ipsec

```
encryption ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>
<ENCR-TYPE> [<KEY-TYPE> <ENCR-KEY>]]
no encryption
```

Description

Configures IPsec ESP authentication and encryption for the selected Vlink.

The **no** form of this command removes IPsec ESP authentication and encryption for the selected Vlink.

Parameter	Description
<code>spi <SPI-INDEX></code>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<code><AUTH-TYPE></code>	Specifies the authentication type: md5 or sha1 .
<code><KEY-TYPE></code>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<code><AUTH-KEY></code>	Specifies the authentication key.
<code><ENCR-TYPE></code>	Specifies the encryption type: des , 3des , aes , or null . NOTE: Encryption type aes is considered to be AES128, AES192, or AES256 based on key length.
<code><ENCR-KEY></code>	Specifies the encryption key.



When the authentication key is not provided on the command line, plaintext authentication key prompting occurs upon pressing Enter, followed by encryption type prompting, and finally plaintext encryption key prompting. The entered key characters are masked with asterisks.



When the authentication key and encryption type are provided on the command line but the encryption key is not provided, plaintext encryption key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting area 1 to use IPsec ESP authentication and encryption for Vlink with provided plaintext keys:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5 plaintext F82#
des plaintext Plane#88
```

Setting area 1 to use IPsec ESP authentication and encryption for Vlink with prompted plaintext keys and encryption type:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? des

Enter the IPsec encryption key: *****
```

```
Re-Enter the IPsec encryption key: *****
```

Setting area 1 to use IPsec ESP authentication and encryption for Vlink provided plaintext authentication key and encryption type but prompted plaintext encryption key:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5 plaintext Fx des
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting area 1 to use IPsec ESP authentication for Vlink with a provided plaintext authentication key and null encryption:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5 plaintext Fx null
```

Removing IPsec ESP authentication and encryption for Vlink on area 1:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# no encryption
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

default-information originate

```
default-information originate [metric <METRIC-VALUE>]
no default-information originate [metric <METRIC-VALUE>]
```

Description

Configures OSPFv3 to advertise the default route (::/0) to its neighbors if it is present in the routing table. Optionally, the metric value can be set for default route ::/0. The default value is 1.

The **no** form of this command disables advertisement of the default route.

Parameter	Description
<i>metric</i> <METRIC-VALUE>	Specifies the OSPF metric value for the default route. Optional. Default: 1.

Examples

Setting advertisement of the default route:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# default-information originate
```

Disabling advertisement of the default route:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no default-information originate
```

Setting advertisement of the default route and specifying an optional metric value of 20:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# default-information originate  
switch(config-ospfv3-1)# default-information originate metric 20
```

Disabling advertisement of the default route and setting metric to the default value:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no default-information originate metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Added parameter: metric <METRIC-VALUE>
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

default-information originate always


```
default-information originate always [metric <METRIC-VALUE>]
no default-information originate always [metric <METRIC-VALUE>]
```

Description

Configures OSPFv3 to advertise the default route (::/0) to its neighbors, regardless if it is present in the routing table or not. Optionally, metric can be set for default route ::/0. The default value is 1.

The **no** form of this command disables advertisement of the default route.

Parameter	Description
<i>metric <METRIC-VALUE></i>	Specifies the OSPFv3 metric value for the default route. Default: 1.

Examples

Setting advertisement of the default route:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# default-information originate always
```

Disabling advertisement of the default route:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no default-information originate always
```

Setting advertisement of the default route with metric set to 20:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# default-information originate always metric 20
```

Disabling advertisement of the default route and setting the metric to the default value:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no default-information originate always metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Added parameter: metric <METRIC-VALUE>
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospf-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

graceful-restart

```

graceful-restart
  restart-interval <INTERVAL>
  helper [strict-lsa-check]
  ignore-lost-interface
  no...
```

Description

Configures graceful restart for OSPFv3. By default graceful restart is enabled on the OSPFv3 router.

The **no** form of this command sets the restart interval to the default of 120 seconds or disables helper mode depending on the specified parameters.

Parameter	Description
restart-interval <INTERVAL>	Specifies the time another router waits for this router to gracefully restart and selects the maximum time to wait in seconds. Range: 5 to 1800. Default: 120.
helper	Specifies that the router will participate in the graceful restart of a neighbor router.
strict-lsa-check	(Optional). Use with the helper parameter to enable strict Link state Advertisement (LSA) checking when acting as a restart helper for a restarting peer. NOTE: OSPF neighbors must disable strict LSA checking. If the local node has fewer OSPF interfaces after restarting, then the neighbors that were adjacent on those interfaces will clear up their adjacencies to the restarting node and will send out link state updates to advertise the dropped adjacency. If strict LSA checking is enabled, the restarting router's neighbors will exit helper mode when they receive the updated LSAs and the graceful restart will still fail.
ignore-lost-interface	Enable the restarting router to ignore lost OSPF interfaces during a graceful restart process. This setting should be enabled on a high availability system to ensure a graceful restart completes successfully, even if OSPF-enabled links fail due to High Availability events like a switchover or failover. NOTE: Enabling this setting means that the hitless restart procedures do not strictly follow those defined in <i>RFC 3623, Graceful OSPF Restart</i>.
no	Negate any parameter or return the setting to its default..

Examples

Enabling OSPF graceful restart:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# graceful-restart restart-interval 40  
switch(config-ospfv3-1)# graceful-restart helper strict-lsa-check
```

Enabling the switch to ignore lost OSPF interfaces during a graceful restart process:

```
switch(config)# router ospfv3 1  
switch (config-ospfv3-1)# graceful-restart ignore-lost-interface
```

Setting the restart interval to default, and disabling helper mode:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no graceful-restart restart-interval  
switch(config-ospfv3-1)# no graceful-restart helper
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

hello-interval

```
hello-interval <INTERVAL>  
no hello-interval
```



For proper operation, the hello interval must be shorter than the dead interval.

Description

Sets the time interval between OSPF hello packets for virtual links.

The **no** form of this command sets the hello interval to the default value of 10 seconds for virtual links.

Parameter	Description
<INTERVAL>	Specifies the time interval for the hello interval, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting OSPF virtual links hello interval:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink6)# hello-interval 30
```

Setting OSPF virtual links hello interval to default:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink6)# no hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 area

```
ipv6 ospfv3 <PROCESS-ID> area <AREA-ID>  
no ipv6 ospfv3 <PROCESS-ID> area <area-id>
```

Description

Runs the OSPFv3 protocol on the interface for the area specified.

To move an interface to a new area, unmap the existing area and then associate a new area with the interface.

The **no** form of this command disables OSPF on the interface and removes the interface from the area. Interfaces which have an IP address configured on the network or in a subset of the network, stop participating in the OSPF protocol

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. Area ID in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Area ID as a decimal value. Range: 0-4294967295.
<PROCESS-ID>	Specifies the OSPFv3 process ID. Range: 1 to 65535.

Examples

Setting OSPFv3 network for the area:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 1 area 1
switch(config-if-vlan)# ipv6 ospfv3 1 area 0.0.0.1
```

Disabling OSPFv3 network for the area:

```
switch(config)# interface 1/1/1
switch(config-if-vlan)# no ipv6 ospfv3 1 area 1
switch(config-if-vlan)# no ipv6 ospfv3 1 area 0.0.0.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 authentication null

ipv6 ospfv3 authentication null

Description

Configures null authentication on an interface which disables IPsec authentication.

Examples

Disabling IPsec on interface VLAN 1:

```
switch(config)# interface van 1
switch(config-if-vlan)# ipv6 ospfv3 authentication null
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 authentication ipsec

```
ipv6 ospfv3 authentication ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>]  
no ipv6 ospfv3 authentication
```

Description

Configures IPsec AH authentication. OSPFv3 interfaces that have IPsec configured at the interface context will not use area level IPsec.

The **no** form of this command removes IPsec AH authentication for the specified area.

Parameter	Description
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting interface VLAN **1** to use IPsec authentication with a provided plaintext authentication key:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# ipv6 ospfv3 authentication ipsec spi 256 md5 plaintext  
f82#
```

Setting interface VLAN **4** to use IPsec authentication with a prompted plaintext authentication key:

```
switch(config)# interface vlan 4  
switch(config-if-vlan)# ipv6 ospfv3 authentication ipsec spi 256 md5  
Enter the IPsec authentication key: *****  
Re-Enter the IPsec authentication key: *****
```

Removing IPsec authentication from interface VLAN **1**:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 authentication
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 cost

```
ipv6 ospfv3 cost <INTERFACE-COST>
no ipv6 ospfv3 cost
```

Description

Sets the cost (metric) associated with a particular interface. The interface cost is used as a parameter to calculate the best routes.

The **no** form of this command sets the cost (metric) associated with a particular interface to the default of 1.

Parameter	Description
<INTERFACE-COST>	Specifies the interface cost value. Range: 1 to 65535. Default: 1.

Examples

Setting OSPFv3 interface cost:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 cost 100
```

Setting the OSPFv3 interface cost to default:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 cost
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 dead-interval

```
ipv6 ospfv3 dead-interval <INTERVAL>  
no ipv6 ospfv3 dead-interval
```

Description

Sets the interval after a neighbor is declared dead when no hello packet is received on the OSPFv3 interface.

The **no** form of this command sets the interval after which a neighbor is declared dead, to the default for the OSPFv3 interface. The default value is 40 seconds (generally four times the hello packet interval).

Parameter	Description
<INTERVAL>	Specifies the time interval for the dead interval, in seconds. Range: 1 to 65535. Default: 40.

Examples

Setting OSPFv3 dead interval on the interface:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# ipv6 ospfv3 dead-interval 30
```

Setting OSPFv3 dead interval to default on the interface:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# no ipv6 ospfv3 dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 encryption ipsec

```
ipv6 ospfv3 encryption ipsec spi <SPI-INDEX> <AUTH-TYPE>
    [<KEY-TYPE> <AUTH-KEY> <ENCR-TYPE> [<KEY-TYPE> <ENCR-KEY>]]
no ipv6 ospfv3 encryption
```

Description

Configures IPsec ESP authentication. OSPFv3 interfaces that have IPsec configured at the interface context will not use area level IPsec ESP.

The **no** form of this command removes IPsec ESP for the specified area.

Parameter	Description
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.
<ENCR-TYPE>	Specifies the encryption type: des , 3des , aes , or null . NOTE: Encryption type aes is considered to be AES128, AES192, or AES256 based on key length.
<ENCR-KEY>	Specifies the encryption key.



When the authentication key is not provided on the command line, plaintext authentication key prompting occurs upon pressing Enter, followed by encryption type prompting, and finally plaintext encryption key prompting. The entered key characters are masked with asterisks.



When the authentication key and encryption type are provided on the command line but the encryption key is not provided, plaintext encryption key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting interface VLAN 1 to use IPsec ESP with provided authentication and encryption keys:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 encryption ipsec spi 256 sha1 plaintext F82
des plaintext F82#450b
```

Setting interface VLAN **3** to use IPsec ESP with prompted authentication and encryption keys:

```
switch(config)# interface vlan 3
switch(config-if-vlan)# ipv6 ospfv3 encryption ipsec spi 256 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? des

Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting interface VLAN **4** to use IPsec ESP with provided authentication password and encryption type but a prompted encryption key:

```
switch(config)# interface vlan 4
switch(config-if-vlan)# ipv6 ospfv3 encryption ipsec spi 256 sha1 plaintext F82
des
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting interface VLAN **1** to use IPsec ESP with provided plaintext authentication key and null encryption:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 encryption ipsec spi 256 sha1 plaintext F82
null
```

Removing IPsec from interface VLAN **1**:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 encryption
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 encryption null

ipv6 ospfv3 encryption null

Description

Configures NULL ESP on an interface which disables IPsec ESP.

Examples

Disable IPsec ESP on interface VLAN 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 encryption null
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 hello-interval

ipv6 ospfv3 hello-interval <INTERVAL>
no ipv6 ospfv3 hello-interval

Description

Sets the time interval between OSPFv3 hello packets for the OSPFv3 interface.

The **no** form of this command sets the time interval between OSPFv3 hello packets to the default for the OSPFv3 interface of 10 seconds.

Parameter	Description
<INTERVAL>	Specifies the time interval between hello packets, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting OSPFv3 hello interval on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 hello-interval 30
```

Setting OSPFv3 hello interval to default on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	

ipv6 ospfv3 network

```
ipv6 ospfv3 network {broadcast|point-to-point}
no ipv6 ospfv3 network
```

Description

Configures the network type for the interface. By default the network type is broadcast network.

The **no** form of this command sets the network type for the interface to the system default of broadcast network.

Parameter	Description
broadcast	Specifies the OSPFv3 network type as a broadcast multiaccess network.
point-to-point	Specifies the OSPFv3 network type as a point-to-point network.

Examples

Setting OSPFv3 network type for the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 network broadcast
switch(config-if-vlan)# ipv6 ospfv3 network point-to-point
```

Disabling OSPFv3 network type for the interface to system default of broadcast network:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 network
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 passive

```
ipv6 ospfv3 passive
no ipv6 ospfv3 passive
```

Description

Configures the interface as an OSPFv3 passive interface. With this setting, the interface participates in the OSPF, but does not send or receive OSPF packets on that interface.

The **no** form of this command resets the interface as active. With this setting, the interface starts sending and receiving OSPF packets.

Examples

Setting the interface as OSPFv3 passive interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 passive
```

Setting the interface as OSPFv3 active interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 passive
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3 priority

```
ipv6 ospfv3 priority <number-value>  
no ipv6 ospfv3 priority
```

Description

Sets the OSPFv3 priority for the interface. The larger the numeric value of the priority, the higher the chance it will become the designated router. Setting a priority of 0 makes the router ineligible to become a designated router or back up designated router.

The **no** form of this command sets the OSPFv3 priority for the interface to the default of 1.

Parameter	Description
<number-value>	Specifies the OSPFv3 priority value. Default: 1. Range: 0 to 255.

Examples

Setting the OSPFv3 priority for the interface:

```
switch(config)# interface vlan /1  
switch(config-if-vlan)# ipv6 ospfv3 priority 50
```

Setting the OSPFv3 priority for the interface to the default of 1:

```
switch(config)# interface vlan 1  
switch(config-if-vlan)# no ipv6 ospfv3 priority
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 ospfv3-af retransmit-interval

```
ipv6 ospfv3-af retransmit-interval <seconds>
no ipv6 ospfv3-af retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for the OSPFv3 interface.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default 5 seconds.

Parameter	Description
<seconds>	Specifies the time interval for the retransmit interval, in seconds. Range: 1 to 3600. Default: 5

Examples

Setting OSPFv3 retransmit interval on the interface:

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# ospfv3-af ipv6 retransmit-interval 30
```

Setting OSPFv3 retransmit interval to the default on the interface:

```
switch# configure terminal
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv6 retransmit-interval
switch(config-if)# no ospfv3-af ipv6 retransmit-interval 30
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	

ipv6 ospfv3 shutdown

```
ipv6 ospfv3 shutdown
no ipv6 ospfv3 shutdown
```

Description

Disables OSPFv3 on the interface. The interface state changes to Down. It does not remove the interface from the OSPF area. To remove the interface, use the command **no ip ospf area**.

The **no** form of this command re-enables OSPFv3 on the interface.

Examples

Disabling OSPFv3 on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 shutdown
```

Re-enabling OSPFv3 on the interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 shutdown
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	

ipv6 ospfv3 transit-delay

```
ipv6 ospfv3 transit-delay <DELAY>
no ipv6 ospfv3 transit-delay
```

Description

Sets the time delay in Link state transmission for the OSPFv3 interface.

The **no** form of this command sets the transit delay in Link state transmission to the default of 1 second.

Parameter	Description
<code><DELAY></code>	Specifies the time delay for the transit delay, in seconds. Range: 1 to 3600. Default: 1.

Examples

Setting OSPFv3 transit delay on the interface

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ipv6 ospfv3 transit-delay 30
```

Setting OSPFv3 transit delay to default on the interface

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ipv6 ospfv3 transit-delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

maximum-paths

```
maximum-paths <MAXIMUM>
no maximum-paths
```

Description

Sets the maximum number of ECMP routes that OSPFv3 can support.

The **no** form of this command sets the maximum number of ECMP routes that OSPFv3 can support to the default value of 4.

Parameter	Description
<code><MAXIMUM></code>	Specifies the maximum number of ECMP routes. Range: 1 to 32. Default: 4.

Examples

Setting maximum number of parallel routes:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1) # maximum-paths 32
```

Setting maximum number of parallel paths to the default value of 4:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1) # no maximum-paths
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10	Increased upper limit of range of <MAXIMUM> parameter to 32.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3- <PROCESS-ID>	Administrators or local user group members with execution rights for this command.

max-metric router-lsa

```
max-metric router-lsa [on-startup <INTERVAL>]  
no max-metric router-lsa [on-startup]
```

Description

Sets the protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations. If the on-startup parameter is used, the router is configured to advertise a maximum metric at startup. That is, for the time specified in seconds, or the default value of 600 seconds.

To disable advertisement of the maximum metric, use the **no** form of the command.

The **no** form of this command advertises the normal cost metrics instead of advertising the maximized cost metric. This setting causes the router to be considered in traffic forwarding.

Parameter	Description
on-startup <INTERVAL>	Automatically advertises the stub Router-LSA (or maximize the router-LSA cost metric) for a specified time interval upon OSPFv3 startup. Specifies the time in seconds. Range: 5 to 86400. Default: 600.

Examples

Setting to maximize the cost metrics for Router LSA:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# max-metric router-lsa
switch(config-ospfv3-1)# max-metric router-lsa on-startup 3000
```

Setting to advertise the normal cost metrics instead of advertising the maximized cost metric:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no max-metric router-lsa
switch(config-ospfv3-1)# no max-metric router-lsa on-startup
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

passive-interface default

```
passive-interface default
no passive-interface default
```

Description

Sets all OSPFv3 interfaces as passive.

The **no** form of this command sets all the OSPFv3 interfaces as active.

Examples

Setting OSPFv3-enabled interfaces as passive:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# passive-interface default
```

Setting OSPFv3-enabled interfaces as active:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no passive-interface default
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute {bgp | connected | host-routes | local loopback | static | ripng | ospf  
<PROCESS-ID>}  
                [route-map <ROUTE-MAP-NAME>]  
no redistribute {bgp | connected | host-routes | local loopback | static | ripng | ospf  
<PROCESS-ID>}  
                [route-map <ROUTE-MAP-NAME>]
```

Description

Redistributes routes originating from other protocols, or from another OSPFv3 process, to the current OSPFv3 process.

If a route map is specified, then only the routes that pass the match clause specified in the route map are redistributed to OSPFv3. Configuration is not allowed if the referenced route map has not yet been configured.

If you try to redistribute routes from an OSPFv3 process which is not created, you are prompted to allow the OSPFv3 process to be auto-created before proceeding with redistribution. If you confirm at the prompt, the OSPFv3 process is created with defaults and redistribution configuration applied. If you deny at the prompt, redistribution configuration is skipped.

If command **route-redistribute active-routes-only** has been issued, only the routes from other protocols which are selected for forwarding are considered for redistribution into OSPFv3.

The **no** form of this command disables redistribution of routes to the current OSPFv3 process.

Parameter	Description
bgp	Specifies redistributing BGP (Border Gateway Protocol) routes.
connected	Specifies redistributing connected (directly attached subnet or host).
host-routes	Redistributes ARP entries. ARP entries learnt through EVPN or over VXLAN tunnels are not redistributed. The host-routes parameter is applicable to HPE Aruba Networking 8325, 10000, 8360, and 9300/9300S Switch series only.

Parameter	Description
local loopback	Specifies redistributing local routes of the loopback interface.
static	Specifies redistributing static routes.
ripng	Specifies redistributing RIPng routes.
ospf <PROCESS-ID>	Specifies redistributing routes from the specified OSPFv3 process ID. Range: 1 to 65535.
route-map <ROUTE-MAP-NAME>	Specifies redistribution filtering by route map. To create a route map, use command route-map .

Examples

Redistributing routes to OSPFv3:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# redistribute bgp
switch(config-ospfv3-1)# redistribute bgp route-map BGP_routes
```

```
switch(config-ospfv3-1)# redistribute host-routes
switch(config-ospfv3-1)# redistribute connected
switch(config-ospfv3-1)# redistribute connected route-map connected_routes
switch(config-ospfv3-1)# redistribute local loopback
switch(config-ospfv3-1)# redistribute local loopback route-map local_routes
switch(config-ospfv3-1)# redistribute static
switch(config-ospfv3-1)# redistribute static route-map static_networks
switch(config-ospfv3-1)# redistribute ripng
switch(config-ospfv3-1)# redistribute ripng route-map rip-routes
switch(config-ospfv3-1)# redistribute ospf 2
```

Redistributing ARP entries:

```
switch(config-ospfv3-1)# redistribute host-routes route-map host_routes12
```

Disabling redistributing routes to OSPFv3:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no redistribute bgp
switch(config-ospfv3-1)# no redistribute bgp route-map BGP_routes
```

```
switch(config-ospfv3-1)# no redistribute host-routes
switch(config-ospfv3-1)# no redistribute connected
switch(config-ospfv3-1)# no redistribute connected route-map connected_routes
switch(config-ospfv3-1)# no redistribute local loopback
switch(config-ospfv3-1)# no redistribute local loopback route-map local_routes
switch(config-ospfv3-1)# no redistribute static
switch(config-ospfv3-1)# no redistribute static route-map static_networks
switch(config-ospfv3-1)# no redistribute ripng
switch(config-ospfv3-1)# no redistribute ripng route-map rip-routes
switch(config-ospfv3-1)# no redistribute ospf 2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.13	Added route-map support for host-routes .
10.12	Added information about the host-routes parameter.
10.08	Added route-map support for supported redistribute source-protocols. Updated information and examples.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

reference-bandwidth

```
reference-bandwidth <BANDWIDTH>
no reference-bandwidth
```

Description

Sets the reference bandwidth for OSPFv3. If the OSPFv3 interface cost is not explicitly set, then the cost of all the OSPFv3 interfaces is recalculated based on the reference bandwidth and link speed of the interface.

For VLAN interfaces the calculated link speed value is 1 Gbps (if the OSPFv3 interface cost is not explicitly set).

The **no** form of this command sets the reference bandwidth for OSPF to the default of 100000 Mbps.

Parameter	Description
<BANDWIDTH>	Specifies the reference bandwidth used to calculate the cost of an interface in Mbps. Range: 1 to 4000000. Default: 100000.

Examples

Setting the reference bandwidth:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# reference-bandwidth 40000
```

Setting the reference bandwidth to the default value:

```
switch(config)# router ospf 1
switch(config-ospfv3-1)# no reference-bandwidth
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

retransmit-interval

```
retransmit-interval <INTERVAL>
no retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for virtual links.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default of 5 seconds for virtual links.

Parameter	Description
<INTERVAL>	Specifies the time interval for the retransmit interval, in seconds. Range: 1 to 3600. Default: 5.

Examples

Setting OSPFv3 virtual links retransmit interval:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# retransmit-interval 30
```

Setting OSPFv3 virtual links retransmit interval to default:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no retransmit-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

router-id

```
router-id <ROUTER-ADDRESS>  
no router-id
```

Description

Sets an ID for the router in an IPv4 address format.

The **no** form of this command unconfigures the router-id for the instance and sets the router-id to the default. The router-id is changed to the dynamically selected router-id. The default router-id 0.0.0.0 updates to the routing stack that triggers to auto-elect a router-id based on the highest IP address of loopback interface, or the highest IP address of interfaces.

Parameter	Description
<ROUTER-ADDRESS>	Specifies the router address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Examples

Setting router-id in the OSPFv3 context:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1) # router-id 1.1.1.1
```

Unconfiguring router-id:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1) # no router-id
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

router ospfv3

```
router ospfv3 <PROCESS-ID> [vrf <VRF-NAME>]
no router ospfv3 <PROCESS-ID> [vrf <VRF-NAME>]
```

Description

Creates the OSPFv3 process (if not created already) and enters the router OSPFv3 instance context. Optionally if specified, you can specify a named VRF, or the default VRF if the <vrf-name> is not specified. Only one OSPFv3 process is allowed per VRF.

The **no** form of this command removes the OSPFv3 instance. If a VRF is specified, it removes the OSPF instance from the named VRF, or the default VRF if the <var-name> is not specified.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID. Length: 1 to 65535.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Entering the router OSPFv3 instance:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)#
```

Setting the router OSPFv3 VRF instance:

```
switch(config)# router ospfv3 1 vrf vrf_red
```

Removing the router OSPFv3 instance:

```
switch#(config)# no router ospfv3 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show ipv6 ospfv3

show ipv6 ospfv3 [<PROCESS-ID>] [all-vrfs | vrf <VRF-NAME>]

Description

Shows OSPFv3 information including area, state, and configuration information.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID optionally to show OSPFv3 information for a particular OSPFv3 process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Showing general OSPFv3 configurations:

```
switch# show ipv6 ospfv3 200
VRF : default                               Process : 200
-----
Router ID           : 1.1.1.1                OSPFv3           : Enabled
BFD                 : Disabled                SPF Start Interval : 200 ms
SPF Hold Interval   : 1000 ms                 SPF Max Wait Interval : 5000 ms
LSA Start Interval   : 5000 ms                 LSA Hold Interval   : 1000 ms
LSA Max Wait Interval : 1000 ms                 LSA Arrival Interval : 1000 ms
External LSAs        : 0                      Checksum Sum        : 0
ECMP                 : 4                      Reference Bandwidth  : 100000 Mbps
Area Border          : Yes                    AS Border          : No
GR Status             : Enabled                GR Interval         : 120 sec
GR State              : Inactive                GR Exit Status       : None
GR Helper             : Enabled                GR Strict LSA Check  : Enabled
GR Ignore Lost I/F    : Disabled                Internal Process ID  : 1
Summary address:
  prefix fd00::1/64, advertise, tag 10

Area      Total Active
-----
Normal    2          2
```

```

Stub          0      0

Area   : 0.0.0.0
-----
Area Type           : Normal      Status           : Active
Total Interfaces    : 1           Active Interfaces : 1
Passive Interfaces  : 0           Loopback Interfaces : 0
SPF calculation count : 4
Area ranges:
  fd00::1/64, inter-area, no-advertise
AH Authentication   : SHA1, SPI 256
Number of LSAs      : 5           Checksum Sum       : 99122

Area   : 0.0.0.1
-----
Area Type           : Normal      Status           : Active
Total Interfaces    : 1           Active Interfaces : 1
Passive Interfaces  : 0           Loopback Interfaces : 0

SPF Calculation Count : 4
Area ranges:
  fd00::1/64, inter-area, no-advertise
ESP Authentication   : SHA1
Encryption           : 3DES, SPI 256
Number of LSAs      : 5           Checksum Sum       : 99122

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 border-routers

```
show ipv6 ospfv3 [<PROCESS-ID>] border-routers [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows the OSPFv3 routing table entries for Area Border Router (ABR) and Autonomous System Border Router (ASBR).

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID to show the OSPFv3 routing table entries for ABR and ASBR for the particular OSPFv3 process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 border router information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

On the HPE Aruba Networking 6400 Switch Series, interface identification differs.

Showing OSPFv3 border routers information for VRF **vrf_red**:

```
switch# show ipv6 ospfv3 border-routers vrf vrf_red
VRF : vrf_red      Process ID : 1
      Internal Routing Table
-----

Codes: i - Intra-area route, I - Inter-area route
      Router-ID Cost  Type   Area   SPF  Nexthop                                Interface
i   1.1.1.1    1    ASBR   0.0.0.0  9    fe80::7272:cfff:fe9a:a15d             1/1/2
i   3.3.3.3    1    ASBR   1.1.1.1  9    fe80::7272:cfff:fe1f:d80             ** tunnel1
```

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 interface

```
show ipv6 ospfv3 [<PROCESS-ID>] interface [<INTERFACE-NAME>] [brief]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID optionally to show the OSPFv3

Parameter	Description
	enabled interfaces for the particular OSPFv3 process. Range: 1 to 65535.
<INTERFACE-NAME>	Selects to show information only for the specified OSPFv3-enabled interface.
brief	Include this parameter to display a brief overview of the following OSPF configuration information. - Interface: OSPF interface name. - Area: OSPF area ID. - Cost: The metric OSPF uses to judge a path's feasibility, calculated as (reference bandwidth / interface bandwidth). - State: Indicates if the interface is a designated router (Dr) or a backup designated router (Backup-dr). - Status: Indicates if the interface is up or down. - Flags: P - Passive A - Active.
all-vrfs	Select to show OSPF-enabled interface information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 information for all interfaces in default VRF:

```
switch# show ipv6 ospfv3 interface
Codes: DR - Designated router  BDR - Backup Designated router

Interface 1/3/10 is Up, Line Protocol is Up
-----
VRF                : default                Process                : 1
IPv6 address       : fe80::9020:c203:280a:e800 Area                :
0.0.0.0
Status             : Up                    Network Type          :
Broadcast
Hello Interval     : 10 sec                Dead Interval          : 40
sec
Transit Delay      : 1 sec                Retransmit Interval    : 5
sec
BFD                : Disabled              Link Speed             : 1000
Mbps
Cost Configured    : NA                    Cost Calculated        : 100
State/Type         : DR                    Router Priority         : 2
DR                 : 1.1.1.1                BDR                    :
2.2.2.2
Link LSAs          : 2                    Checksum Sum           :
39245
Authentication     : no                    Passive                : No

Codes: DR - Designated router  BDR - Backup Designated router

Interface 1/3/11 is Up, Line Protocol is Up
-----
VRF                : default                Process                : 1
IPv6 address       : fe80::9020:c203:2c0a:e800 Area                :
0.0.0.1
Status             : Up                    Network Type          :
```

```

Broadcast
Hello Interval      : 10      sec      Dead Interval      : 40
sec
Transit Delay       : 1       sec      Retransmit Interval : 5
sec
BFD                 : Disabled      Link Speed         : 1000
Mbps
Cost Configured     : NA           Cost Calculated    : 100
State/Type          : BDR          Router Priority     : 1
DR                  : 3.3.3.3      BDR                :
1.1.1.1
Link LSAs           : 2           Checksum Sum       :
83119
Authentication      : no          Passive            : No

```

Showing overview information for OSPFv3 enabled interfaces for all VRFs in brief:

```

switch# show ipv6 ospfv3 interface brief all-vrfs
VRF : default                      Process : 1
=====

Total Number of Interfaces: 2

Flags: P - Passive  A - Active

Interface      Area              Cost      State      Status      Flags
-----
1/3/10         0.0.0.0           100       DR         Up          A
1/3/11         0.0.0.1           100       BDR        Up          A

```

Showing overview information for OSPFv3 enabled interfaces for all VRFs:

```

6200(config)# show ipv6 ospfv3 interface br all-vrfs
VRF : default                      Process : 1
=====

Total Number of Interfaces: 1

Flags: P - Passive  A - Active

Interface      Area              Cost      State      Status      Flags
-----
1/1/1          0.0.0.0           100       BDR        Up          A

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.09	Output of the show ipv6 ospfv3 interface command includes

Release	Modification
	flags to indicate whether the interface is in passive or active mode.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 lsdb

```
show ipv6 ospfv3 [<process-id>] lsdb
  adv-router {<ROUTER-ID>|self}
  area <AREA-ID>
  lsid <link-state-id>
  all-vrfs|vrf <VRF-NAME>{
    as-external
    asbr-summary
    database-summary
    inter-area-prefix
    inter-area-router
    intra-area-prefix
    link
    network
    nssa-external
    router
    summary
  }
  vsx-peer
```

Description

Shows the OSPFv3 link state database summary for different OSPF LSAs (Link State Advertisement). Use the parameters to get information for a particular LSA.

Parameter	Description
<PROCESS-ID>	Enter an OSPFv3 process ID to display general OSPF information for a particular OSPF process. Range: 1 to 65535.
adv-router {<ROUTER-ID> self}	Select to display link states for a particular advertising router. Specify either a Router ID of the advertising router or specify self to show self-originated link states.
area <AREA-ID>	Select to display information filtered for the specified area in one of the following formats. OSPFv3 area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPFv3 area identifier in decimal format. Value: 0 to 4294967295.

Parameter	Description
<code>lsid <LINK-STATE-ID></code>	Select to display information filtered by link state identifier specified in IPv4 address format (A.B.C.D).
<code>all-vrfs {vrf <vrf-name>}</code>	Select all-vrfs to display general OSPF information for all VRFs, or use the vrf <VRF-NAME> option to display information for a specific VRF. Optionally select one of the following parameters to filter the link state database information.
<code>as-external</code>	Show external link states (LSA type 5)
<code>database-summary</code>	Select to display the count of each type of LSA and each area in the database. NOTE: The database-summary parameter does not support the area <area-id> , lsid <link-state-id> or adv-router {<router-id> self} parameters.
<code>inter-area-prefix</code>	Show inter-area prefix link states (LSA type 3)
<code>inter-area-router</code>	Show inter-area router link states (LSA type 4)
<code>intra-area-prefix</code>	Show intra-area prefix link states (LSA type 9)
<code>link</code>	Show link states (LSA type 8)
<code>network</code>	Show network LSAs (LSA type 2).
<code>nssa-external</code>	Show NSSA external link states (LSA type 7).
<code>router</code>	Show router LSAs (LSA type 1).
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing OSPFv3 link state database (LSDB) general information:

```
switch# show ipv6 ospfv3 lsdb
OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
-----
ADV Router    Age      Seq#      Checksum    LSID        Link Count  Bits
-----
40.40.40.40   930     0x80000004 0x2ea1      0           3           None
50.50.50.50   935     0x80000002 0x8b52      0           1           E
60.60.60.60   943     0x800003c5 0x9854      0           2           None

Network Link State Advertisements (Area 0.0.0.0)
-----
ADV Router    Age      Seq#      Checksum    LSID        Router Count
```



```

-----
60.60.60.60      944      0x80000001  0x7179      1360007168  2
50.50.50.50      935      0x80000001  0x516a      19          1

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40     929      0x80000001  0x2498      131072    FEC0:3344::/32
50.50.50.50     928      0x80000001  0x5b2f      65536     111::/64

Inter Area Router Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Destination Router ID
-----
40.40.40.40     929      0x80000001  0x2498      1         33.33.33.33

AS External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40     264      0x80000001  0x24cc4     1         10::/64
40.40.40.40     675      0x80000001  0x5b00f     2         11::/64

NSSA External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
3.3.3.3         264      0x80000001  0x24ac2     1         200::/64

Link-local Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Interface
-----
50.50.50.50     264      0x80000001  0x653c4     19        1/1/1

Intra Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
-----
ADV Router      Age      Seq#      Checksum    LSID      Referenced LS Type
Referenced LSID
-----
-----
50.50.50.50     263      0x80000001  0x1da34     1         0x2001          0
50.50.50.50     264      0x80000001  0x2a45d     1         0x2002          19

```

Showing AS external link states:

```

switch# show ipv6 ospfv3 lsd as-external
OSPF Router with ID (60.60.60.60) (Process ID 1 VRF default)
=====

AS External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40     264      0x80000001  0x24cc4     1         10::/64
40.40.40.40     675      0x80000001  0x5b00f     2         11::/64

```

Showing the LSDB database summary:

```
switch# show ipv6 ospfv3 lsd database-summary
OSPF Router with ID (10.1.1.1) (Process ID 1 VRF default)
=====

Area 0.0.0.0 database summary
-----
LSA Type                Count
-----
Router                   2
Network                  1
Inter Area Prefix        1
Inter Area Router        0
NSSA External            0
Link                     3
Intra Area Prefix        3
-----
Total                    10

Process 1 database summary
-----
LSA Type                Count
-----
Router                   2
Network                  1
Inter Area Prefix        1
Inter Area Router        0
AS External              2
NSSA External            0
Link                     3
Intra Area Prefix        3
-----
Total                    12
```

Showing inter-area prefix LSAs:

```
switch# show ipv6 ospfv3 lsd inter-area-prefix
OSPF Router with ID (6.6.6.6) (Process ID 1 VRF default)
=====

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router    Age    Seq#    Checksum    LSID    Prefix
-----
40.40.40.40   929    0x80000001  0x2498     131072  FEC0:3344::/32
50.50.50.50   928    0x80000001  0x5b2f     65536   111::/64
```

Showing network LSAs:

```
switch# show ipv6 ospfv3 lsd network
OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Network Link State Advertisements (Area 0.0.0.0)
-----
ADV Router    Age    Seq#    Checksum    LSID    Router Count
-----
60.60.60.60   944    0x80000001  0x7179     1360007168  2
50.50.50.50   935    0x80000001  0x516a     19         1
```

Showing NSSA external link states:

```
switch# show ipv6 ospfv3 lsdn nssa-external
OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

NSSA External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
3.3.3.3         264     0x80000001 0x24ac2     1         200::/64
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 neighbors

```
show ipv6 ospfv3 [<PROCESS-ID>] neighbors [<NEIGHBOR-ID>]
[interface <INTERFACE-NAME>] [detail | summary]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 neighbors.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID to show OSPFv3 neighbor information for the particular OSPFv3 process. Range: 1 to 65535.
neighbors <NEIGHBOR-ID>	Shows information about a particular neighbor, specified in IPv4 format (A.B.C.D).
interface <INTERFACE-NAME>	Shows neighbor information only for the specified interface.
detail	Shows detailed information for the neighbors.
summary	Shows summary information for the neighbors.
all-vrfs	Shows neighbor information for all VRFs.

Parameter	Description
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 neighbors information:

Showing OSPFv3 neighbors information for a specific neighbor:

```
switch# show ipv6 ospfv3 neighbors 3.3.3.3
VRF : default                      Process : 1
-----
Router-Id      : 3.3.3.3           Area          : 0.0.0.0
Interface     : 1/1/1             Address        :
fe80::7272:cfff:fe79:7510
State         : FULL              Neighbor Priority : 1
Dead Timer Due : 00:00:36         Options       : 0x13
Time since last state change : 00h:14m:45s
```

Showing detail OSPFv3 neighbors information for a specific neighbor:

```
switch# show ipv6 ospfv3 neighbors 2.2.2.2 detail
VRF : default                      Process : 1
-----
Router-Id      : 3.3.3.3           Area          : 0.0.0.0
Interface     : 1/1/1             Address        :
fe80::7272:cfff:fe79:7510
State         : FULL              Neighbor Priority : 1
DR            : 3.3.3.3           BDR           : 1.1.1.3
Dead Timer Due : 00:00:36         Options       : 0x13
Retransmission Queue Length : 0
Time Since Last State Change : 00h:14m:45s
```

Showing OSPFv3 neighbors information for interface **1/1/1**:

```
switch# show ipv6 ospfv3 neighbors 3.3.3.3 interface 1/1/1
VRF : default                      Process : 1
-----
Router-Id      : 3.3.3.3           Area          : 0.0.0.0
Interface     : 1/1/1             Address        :
fe80::7272:cfff:fe79:7510
State         : FULL              Neighbor Priority : 1
Dead Timer Due : 00:00:36         Options       : 0x13
Time Since Last State Change : 00h:14m:45s
```

Showing summary OSPFv3 neighbors information for a specific neighbor for all VRFs:

```
switch# show ipv6 ospfv3 neighbors 3.3.3.3 summary all-vrfs
OSPFv3 Process ID 1 VRF default, Neighbor Summary
=====
Interface      Down Attempt Init TwoWay ExStart Exchange Loading Full Total
-----
1/1/1          0    0      0    0      0      0      0      1    1
```

```

Total          0    0    0    0    0    0    0    1    1

OSPFv3 Process ID 1 VRF red, Neighbor Summary
=====

Interface      Down Attempt Init TwoWay ExStart Exchange Loading Full Total
-----
1/1/2          0    0    0    0    0    0    0    1    1
Total          0    0    0    0    0    0    0    1    1

```

Showing OSPFv3 neighbors information for VRF red:

```

switch# show ipv6 ospfv3 neighbors vrf red
OSPFv3 Process ID 2 VRF red
=====

Total Number of Neighbors: 1

Neighbor ID      Priority  State           Interface
-----
4.4.4.4          1        FULL/DR         1/1/2
Neighbor address fe80::7272:cfff:fe79:7510

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 routes

```

show ipv6 ospfv3 [<PROCESS-ID>] routes [<PREFIX/LENGTH>]
[all-vrfs | vrf <VRF-NAME>]

```

Description

Shows the OSPFv3 routing table information.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID that shows information from the OSPFv3 routing table for the particular OSPFv3 process. Range: 1 to 65535.
<PREFIX/LENGTH>	Specifies the IPv6 destination prefix showing information about a particular destination prefix. For example, 2010:bd9::/32.
all-vrfs	Select to show OSPFv3 routing table information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 routing table information:

```
switch# show ipv6 ospfv3 routes
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPFv3 Process ID 1 VRF default, Routing Table
-----

Total Number of OSPFv3 Routes : 2

111::/64          (i) area:0.0.0.0
    directly attached to interface 1/1/1, cost 1 distance 110
fd00::/64         (i) area:0.0.0.1
    directly attached to interface vlan10, cost 1 distance 110
```

Showing OSPFv3 routing table information for VRF red:

```
switch# show ipv6 ospfv3 routes vrf red

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPFv3 Process ID 2 VRF red, Routing Table
-----

Total Number of OSPFv3 Routes : 1

222::/64          (i) area:0.0.0.1
    directly attached to interface 1/1/2, cost 1 distance 110
```

Showing OSPFv3 routing table information for destination prefix fd00::/64:

```
switch# show ipv6 ospfv3 1 routes fd00::/64
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

OSPFv3 Process ID 1 VRF default, Routing Table for prefixes fd00::/64
-----

Total Number of OSPFv3 Routes : 1
```

```
fd00::/64          (i) area:0.0.0.1
                    directly attached to interface vlan10, cost 1 distance 110
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 statistics

```
show ipv6 ospfv3 [<PROCESS-ID>] statistics
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows OSPFv3 statistics.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID that shows information on the OSPFv3 SPF statistics for the particular OSPFv3 process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 SPF statistics information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 statistics information:

```
switch# show ipv6 ospfv3 statistics
OSPFv3 Process ID 1 VRF default, Statistics (cleared 3h 2m 21s ago)
-----
Unknown Interface Drops           : 0
Unknown Virtual Interface Drops   : 0
Bad IPv6 Header Length Drops      : 0
Wrong OSPFv3 Version Drops        : 0
```

```
Bad Source IPv6 Drops      : 0
Resource Failure Drops     : 0
Bad Header Length Drops   : 0
Total Drops                : 0
```

Showing OSPFv3 statistics information for VRF red:

```
switch# show ipv6 ospfv3 2 statistics vrf red

OSPFv3 Process ID 2 VRF red, Statistics (cleared 3h 2m 30s ago)
-----

Unknown Interface Drops      : 0
Unknown Virtual Interface Drops : 0
Bad IPv6 Header Length Drops : 0
Wrong OSPFv3 Version Drops   : 0
Bad Source IPv6 Drops        : 0
Resource Failure Drops       : 0
Bad Header Length Drops      : 0
Total Drops                  : 0
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 statistics interface

```
show ipv6 ospfv3 [<PROCESS-ID>] statistics interface [<INTERFACE-NAME>]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows the OSPFv3 statistics for the OSPFv3-enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 process ID to show OSPF-enabled interface statistics information on the specified OSPFv3 process. Range: 1

Parameter	Description
	to 65535.
<INTERFACE-NAME>	Selects to show information only for the specified interface.
all-vrfs	Select to show OSPF-enabled interface statistics information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Showing OSPFv3-enabled interfaces information for interface 1/1/1:

```
switch# show ipv6 ospfv3 statistics interface all-vrfs
OSPFv3 Process ID 1 VRF default, Interface vlan2000 Statistics (cleared 0h 2m 52s
ago)

=====
====

Tx Hello packets      : 0                Rx Hello packets      : 0
Tx Hello bytes        : 0                Rx Hello bytes        : 0
Tx DD packets         : 0                Rx DD packets         : 0
Tx DD bytes           : 0                Rx DD bytes           : 0
Tx LS request packets : 0                Rx LS request packets : 0
Tx LS request bytes   : 0                Rx LS request bytes   : 0
Tx LS update packets  : 0                Rx LS update packets  : 0
Tx LS update bytes    : 0                Rx LS update bytes    : 0
Tx LS ack packets     : 0                Rx LS ack packets     : 0
Tx LS ack bytes       : 0                Rx LS ack bytes       : 0

Total IPsec packets processed : 0
Total IPsec bytes processed   : 0
Total Number of State Changes : 0
Number of LSAs                : 0
LSA Checksum Sum              : 0

Total OSPFv3 Packets Discarded: 0
-----

Reason                      Packets Dropped
-----
Invalid Type                 0
Invalid Length               0
Invalid Version              0
Bad or Unknown Source        0
Area Mismatch                0
Self-originated              0
Duplicate Router ID          0
Interface Standby            0
Total Hello Packets Dropped  0
  Hello Interval Mismatch    0
  Dead Interval Mismatch     0
  Options Mismatch           0
  MTU Mismatch               0
  Neighbor Ignored           0
Resource Failures            0
Bad LSA Length               0
Others                       0
```

```
IPsec Authentication Errors      0
IPsec ESP Errors                 0

Total LSAs Ignored : 0
-----
Bad Type           : 0
Bad Length         : 0
Invalid Data       : 0
Invalid Checksum   : 0
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 ospfv3 virtual-links

```
show ipv6 ospfv3 [<PROCESS-ID>] virtual-links [brief]
[all-vrfs | vrf <vrf-name>]
```

Description

Displays the current state and parameters of the OSPFv3 virtual links.

Parameter	Description
<PROCESS-ID>	Enter an OSPFv3 process ID to display information on the OSPFv3 virtual links for the particular OSPFv3 process. Range: 1 to 65535.
brief	Select to display brief overview information for the OSPFv3 virtual links.
all-vrfs	Select to display OSPFv3 virtual links information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Show OSPFv3 virtual links information:

```
switch# show ipv6 ospfv3 virtual-links
Virtual link to router 4.4.4.4 is down
-----

Process ID 1 VRF default, Transit area 0.0.0.1
Transit delay 1 sec
Timer Intervals: hello 10, dead 40, retransmit 5
Number of Link LSAs: 0, checksum sum 0
0 state changes
AH Authentication: MD5, SPI: 256
```

Show brief overview information for OSPFv3 virtual links:

```
switch# show ospfv3 virtual-links brief
OSPFv3 Process ID 1 VRF default
=====

Total Number of Virtual Links: 1

Remote Router      Transit Area      Status
-----
4.4.4.4           0.0.0.1          down
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

summary-address

```
summary-address <IPV6-ADDR>/<MASK> [no-advertise | tag <TAG-VALUE>]
no summary-address <prefix/length> [no-advertise | tag <tag-value>]
```

Description

Summarizes the external routes with the matching address and mask. When advertising this route, its metric is set to the lowest cost path from among the routes that were summarized.

The **no** form of this command disables route summarization.



This command only works for an ASBR (Autonomous System Boundary Router).

Parameter	Description
<IPv6-ADDR>	Specifies an IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
no-advertise	Do not advertise the aggregate route. Suppress routes that match the specified prefix/mask pair.
tag <TAG-VALUE>	Specify the tag for the aggregate route. The summary prefix will be advertised along with the tag value in External LSAs. Range: 0 to 4294967295

Examples

Setting OSPF route summarization:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# summary-address 2001:DB8::1/32
```

Disabling route summarization:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no summary-address 2001:DB8::1/32
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

timers lsa-arrival

```
timers lsa-arrival <DELAY>
no timers lsa-arrival
```

Description

Configures the minimum delay between receiving the same LSA from a peer. The same LSA is an LSA that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same

LSA arrives sooner before the delay expires, the LSA is dropped. Generally, the LSA arrival timer should be set to a value less than or equal to the start-time value for the command **timers throttle lsa start** on the neighbor.

The **no** form of this command sets the LSA timers to default values.

Parameter	Description
<DELAY>	Specifies the delay in milliseconds. Range: 0 to 600000. Default: 1000.

Examples

Setting the LSA arrival timer:

```
switch(config)# router ospf 1  
switch(config-ospfv3-1)# timers lsa-arrival 10
```

Setting the LSA arrival timer to default:

```
switch(config)# router ospf 1  
switch(config-ospfv3-1)# no timers lsa-arrival
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

timers throttle lsa

```
timers throttle lsa start-time <START-TIME> hold-time <HOLD-TIME> max-wait-time <WAIT-TIME>  
no timers throttle lsa
```

Description

Configures the timers for LSA generation.

The **no** form of this command sets the LSA timers to default values.

Parameter	Description
<code>start-time <START-TIME></code>	Specifies the initial wait time in milliseconds after which LSAs are generated. When set to 0, the LSAs are generated without any delay. Range: 0 to 600000. Default: 5000.
<code>hold-time <HOLD-TIME></code>	Specifies the amount of time, in milliseconds, between regeneration of an LSA. The hold time doubles each time the same LSA must be regenerated, until max-wait-time is reached. When set to 0, LSA regeneration time is not increased. Range: 0 to 600000. Default: 0.
<code>max-wait-time <WAIT-TIME></code>	Specifies the maximum wait time, in milliseconds, for regeneration of the same LSA. When set to 0, LSA regeneration time is not increased. Range: 0 to 600000. Default: 0.

Examples

Setting the LSA timers:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# timers throttle lsa start-time 100 hold-time 1000 max-wait-time 10000
```

Setting LSA timers to default values:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no timers throttle lsa
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospfv3-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

timers throttle spf

```
timers throttle spf start-time <START-TIME> hold-time <HOLD-TIME>
max-wait-time <WAIT-TIME>
no timers throttle spf
```

Description

Configures timers for SPF calculation. There are three timers:

- **start-time** Is the initial delay before an SPF calculation is started. Default is 200 milliseconds.
- **hold-time** Is the progressive backoff time to wait before next scheduled SPF calculation. Default is 1000 milliseconds. If a route change event occurs during this period, the value doubles until it reaches the *max-wait-time*.
- **max-wait-time** Is the maximum time to wait before the next scheduled SPF calculation. Default is 5000 milliseconds. This is used to limit the SPF hold timer and also defines the time to be considered for which the OSPF LSDB has to be stable, after which the SPF throttle mechanism is reset.

The **no** form of this command sets all the configured non-default timers to default value.

Parameter	Description
<code><START-TIME></code>	Time in milliseconds to set timer for initial SPF delay. Default: 200.
<code><HOLD-TIME></code>	Time in milliseconds to set the minimum hold time between two consecutive SPF calculations. Default: 1000.
<code><WAIT-TIME></code>	Time in milliseconds to set the maximum wait time between two consecutive SPF calculations. Default: 5000.

Examples

Setting non-default timer values for SPF throttling:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# timers throttling spf start-time 500 hold-time 3000 max-
wait-time 9000
Switch(config-ospfv3-1)# show running-config current-context
router ospfv3 1
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2 nssa no-summary
    area 0.0.0.3 stub
```

Setting default timer values for SPF throttling after configuring non-default values:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# no timers throttling spf
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

transit-delay

```
transit-delay <DELAY>
no transit-delay
```

Description

Sets the time delay in Link state transmission for virtual links.

The **no** form of this command sets the delay in Link state transmission to the default of 1 second for virtual links.

Parameter	Description
<DELAY>	Specifies the time delay for the transit delay, in seconds. Range: 1 to 3600. Default: 1.

Examples

Setting OSPFv3 virtual links transit delay:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# transit-delay 30
```

Setting OSPFv3 virtual links transit delay to default:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no transit-delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

trap-enable

trap-enable
no trap-enable

Description

Enables the notification of the events to be sent as traps to the SNMP management stations for OSPFv3. The **no** form of this command disables the notification of the events to be sent as traps to the SNMP management stations for OSPFv3.

Examples

Enabling sending notification of events as traps:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# trap-enable
```

Disabling sending notification of events as traps:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-1)# no trap-enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

OSPFv3 AF commands

active-backbone stub-default-route

active-backbone stub-default-route

Description

This command enables the router to send a default route to stub areas if there is an active loopback link in the backbone area. The configuration is not required if backbone area has neighbors or passive interfaces configured. By default, active backbone detection is disabled.

Parameter	Description
<i>stub-default-route</i>	Advertise default route to stub if loopback in backbone area.

Examples

Enabling the router to send an IPv4 default route to stub areas:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# active-backbone stub-default-route
```

Enabling the router to send an IPv6 default route to stub areas:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# active-backbone stub-default-route
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

address-family unicast

address-family { <ipv4> | <ipv6> } unicast

Description

This command specifies the IPv4/IPv6, address-family and enters address family configuration mode.

Examples

Specifying an IPv4 address-family:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
```

Specifying an IPv6 address-family:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv6 unicast
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-af- <i><PROCESS-ID></i>	Administrators or local user group members with execution rights for this command.

area default-metric

```
area <AREA-ID> default-metric <METRIC>  
no area <AREA-ID> default-metric
```

Description

Sets the cost of default-summary LSAs announced to the stub/nssa areas.

The **no** form of this command resets the cost of the default-summary LSAs announced to stub/nssa areas to the default of 1.

Parameter	Description
<i><AREA-ID></i>	Specifies the area ID as one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
default-metric <i><METRIC></i>	Specifies the default metric of default-summary LSAs announced to the stub/nssa areas, to the specified value. Default: 1. Range: 0 to 16777215.

Examples

Setting cost for default IPv4 LSA summary:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv4 unicast  
switch(config-ospfv3-ipv4-uc)# area 1 default-metric 2  
switch(config-ospfv3-ipv4-uc)# area 1.1.1.1 default-metric 2
```

Setting cost for default IPv4 LSA summary to default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no area 1 default-metric
switch(config-ospfv3-ipv4-uc)# no area 0.0.0.1 default-metric
switch(config-ospfv3-ipv4-uc)# no area 0.0.0.1 default-metric 2
```

Setting cost for default IPv6 LSA summary:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1 default-metric 2
switch(config-ospfv3-ipv6-uc)# area 1.1.1.1 default-metric 2
```

Setting cost for default IPv6 LSA summary to default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# no area 1 default-metric
switch(config-ospfv3-ipv6-uc)# no area 0.0.0.1 default-metric
switch(config-ospfv3-ipv6-uc)# no area 0.0.0.1 default-metric 2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

area nssa

```
area <AREA-ID> nssa [no-summary]
no area <AREA-ID> nssa [no-summary]
```

Description

This command sets the area type as NSSA. If area is present and not NSSA area, changes the area type to NSSA area. If **no-summary** is configured the area type will be NSSA No-Summary.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a

Parameter	Description
	decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295. <i>Required</i>
nssa	Configure OSPFv3 AF area as NSSA. <i>Required</i>
no-summary	Do not inject inter-area routes into NSSA. <i>Optional</i>
no	Unsets the area type as NSSA. This means that the configured area becomes an area type default. The no area area-id nssa no-summary command will stop sending Area Border Router(ABR) summary link advertisements into the NSSA area, but will not unset the area as NSSA. <i>Optional</i>

Examples

Creating an NSSA area for OSPFv3 AF:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# area 1 nssa
switch(config-ospfv3-ipv4-uc)# area 1 nssa no-summary
```

Clearing the NSSA area for OSPFv3 AF:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# no area 1 nssa
switch(config-ospfv3-ipv6-uc)# no area 1 nssa no-summary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID> config-ospfv3-ipv6-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area

```
area <AREA-ID>
no area <AREA-ID>
```

Description

Creates a normal area with **<AREA-ID>** set if not present. If area is present and is not the normal area, this command changes the area type to normal area.

The **no** form of this command deletes the area with the **<AREA-ID>** specified. The area can be of any type (stub, stub no-summary, and default normal area).

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPFv3 AF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPFv3 AF area identifier in decimal format. Range: 0 to 4294967295.

Examples

Creating an IPv4 normal area:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# area 1
switch(config-ospfv3-ipv4-uc)# area 1.1.1.1
```

Creating an IPv6 normal area:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1
switch(config-ospfv3-ipv6-uc)# area 1.1.1.1
```

Deleting an IPv4 area:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no area 1
switch(config-ospfv3-ipv4-uc)# no area 0.0.0.1
```

Deleting an IPv6 area:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# no area 1
switch(config-ospfv3-ipv6-uc)# no area 1.1.1.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

area range

```
area <AREA-ID> range <IP-PREFIX> type {inter-area | nssa} [no-advertise]
no area <AREA-ID> range <IP-PREFIX> type {inter-area | nssa} [no-advertise]
```

Description

Summarizes the routes with the matching address or masks for OSPFv3 AF. This command only works for border routers.

The **no** form of this command unsets the route summarization for the configured IP prefix address on the ABR. When using the **no** form of the command with the **no-advertise** option, enables advertising this range to other areas.

Parameter	Description
<AREA-ID>	Specifies the area identifier as one of the following formats. OSPFv3 AF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPFv3 AF area identifier in decimal format. Range: 0 to 4294967295.
range <IP-PREFIX>	Specifies summarizing routes matching the area range prefix/mask in IPv4 or IPv6 format.
type {inter-area nssa}	Specifies the type this address aggregation applies to as either inter-area range prefix or NSSA range prefix.
no-advertise	Specifies the address range status as DoNotAdvertise (do not advertise this range to other areas).

Examples

Summarizing inter-area or NSSA paths on OSPFv3 AF for IPv4:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# area 1 range 10.1.0.0/16 type inter-area
switch(config-ospfv3-ipv4-uc)# area 1 range 10.1.0.0/16 type inter-area no
advertise
switch(config-ospfv3-ipv4-uc)# area 1 range 10.1.0.0/16 type nssa
switch(config-ospfv3-ipv4-uc)# area 1 range 10.1.0.0/16 type nssa no-advertise
```

Unsetting summarization on OSPFv3 AF for IPv4:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no area 1 range 10.1.0.0/16 type inter-area
switch(config-ospfv3-ipv4-uc)# no area 1 range 10.1.0.0/16 type inter-area no
advertise
switch(config-ospfv3-ipv4-uc)# no area 1 range 10.1.0.0/16 type nssa
switch(config-ospfv3-ipv4-uc)# no area 1 range 10.1.0.0/16 type nssa no-advertise
```

Summarizing inter-area or NSSA paths on OSPFv3 AF for IPv6:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1 range fd00::1/64 type inter-area
switch(config-ospfv3-ipv6-uc)# area 1 range fd00::1/64 type inter-area no
advertise
switch(config-ospfv3-ipv6-uc)# area 1 range fd00::1/64 type nssa
switch(config-ospfv3-ipv6-uc)# area 1 range fd00::1/64 type nssa no-advertise
```

Unsetting summarization on OSPFv3 AF for IPv6:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# no area 1 range fd00::1/64 type inter-area
switch(config-ospfv3-ipv6-uc)# no area 1 range fd00::1/64 type inter-area no
advertise
switch(config-ospfv3-ipv6-uc)# no area 1 range fd00::1/64 type nssa
switch(config-ospfv3-ipv6-uc)# no area 1 range fd00::1/64 type nssa no-advertise
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID> config-ospfv3-ipv6-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

area stub

```
area <AREA-ID> stub [no-summary]
no area <AREA-ID> stub [no-summary]
```

Description

Creates the stub area with <AREA-ID> if not present. If area is present and is not the stub area, this command changes the area type to stub area. If **no-summary** is used, area type will be totally stubby area.

The **no** form of this command unsets the area type as stub. The configured area will be changed to the default normal area. The **no area <AREA-ID> stub no-summary** command will start sending Area Border Router (ABR) summary link advertisements into the stub area, but will not unset the stub area.



ABR does not inject the default route in a Totally Stubby Area with loopback in Area 0.0.0.0. As a workaround, configure a passive interface or active neighbors in the backbone area.

Parameter	Description
<AREA-ID>	Specifies the area ID as one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
stub [no-summary]	Specifies stub area type. If area is present and not stub area, this parameter changes the area type to stub area. If no-summary is specified, area type will be totally stubby area, which means do not inject inter-area routes into stub.

Examples

Creating an IPv4 stub area:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# area 1 stub
switch(config-ospfv3-ipv4-uc)# area 1 stub no-summary
```

Unsetting the IPv4 stub area type:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc) # no area 1 stub
switch(config-ospfv3-ipv4-uc) # no area 1 sub no-summary
```

Creating an IPv6 stub area:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1 stub
switch(config-ospfv3-ipv6-uc)# area 1 stub no-summary
```

Unsetting the IPv6 stub area type:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc) # no area 1 stub
switch(config-ospfv3-ipv6-uc) # no area 1 sub no-summary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

area virtual-link

```
area <AREA-ID> virtual-link <ROUTER-ID>
no area <AREA-ID> virtual-link <ROUTER-ID>
```

Description

Creates an OSPF virtual link with remote ABR (if not created already) and enters the vlink context. The configuration is supported only in ipv6-unicast address-family.

The **no** form of this command deletes an OSPF virtual link with the specified router ID of the remote ABR. If no **<ROUTER-ID>** is specified, the **no** form of the command sets the virtual link to the default settings.

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. OSPF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPF area identifier in decimal format. Range: 0 to 4294967295.
virtual-link <ROUTER-ID>	Configures a virtual link with the specified router ID of the remote ABR.

Examples

Configuring OSPFv3 AF virtual links:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
```

Deleting OSPFv3 AF virtual links:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
```

```
switch(config-ospfv3-ipv6-uc)# no area 100 virtual-link 100.0.1.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

authentication ipsec spi

```
authentication ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>]  
no authentication
```

Description

Configures IPsec AH authentication for the selected Vlink.

The **no** form of this command removes IPsec AH authentication for the selected Vlink.

Parameter	Description
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting area 1 to use IPsec AH authentication for Vlink with provided plaintext key:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# authentication ipsec spi 256 sha1 plaintext abcd
```

Setting area 1 to use IPsec AH authentication for Vlink with prompted plaintext key:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# authentication ipsec spi 256 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Removing IPsec AH authentication for Vlink on area 1:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# no authentication
switch(config-router-vlink6)# no authentication ipsec spi 1234 md5 ciphertext
qwertyuioplkjhgfdasazxcvbnmkjhgfdsa
switch(config-router-vlink6)# no authentication ipsec spi 1234 sha1 ciphertext
qwertyuioplkjhgfdasazxcvbnmkjhgfdsa
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

clear ospfv3-af ipv4 neighbor

```
clear ospfv3-af [<PROCESS-ID>] ipv4 neighbor [<NEIGHBOR-ID>] [interface <INTERFACE-NAME>
| vlan <VLAN-ID> | lag <LAG-ID>] | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>] [all-vrfs
| vrf <VRF-NAME>]
```

Description

Resets the neighbor and clears the OSPFv3 AF neighbor information.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv3 AF process ID to clear the statistics for the particular OSPFv3 AF process. Range: 1 to 65535.
neighbor <NEIGHBOR-ID>	Specifies the router ID of a neighbor.
interface <INTERFACE-NAME>	Specifies the OSPFv3 AF statistics to clear for the specified interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
all-vrfs	Select to clear the OSPFv3 AF statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv3 AF neighbor information:

```
switch# clear ospfv3-af 1 ipv4 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af 1 ipv4 neighbor 3.3.3.3
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af 1 ipv4 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af 1 ipv4 neighbor 3.3.3.3 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv4 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv4 neighbor 5.5.5.5
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv4 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv4 neighbor 5.5.5.5 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear ospfv3-af ipv4 statistics

```
clear ospfv3-af [<PROCESS-ID>] ipv4 statistics [interface [interface <INTERFACE-NAME> |
vlan <VLAN-ID> | lag <LAG-ID>] | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>] [all-vrfs |
vrf <VRF-NAME>]
```

Description

Clears the OSPFv3 AF event statistics.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv3 AF process ID to clear the statistics for the particular OSPFv3 AF process. Range: 1 to 65535.
interface <INTERFACE-NAME>	Specifies the OSPFv3 AF statistics to clear for the specified interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
all-vrfs	Select to clear the OSPFv3 AF statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv3 AF event statistics:

```
switch# clear ospfv3-af ipv4 statistics
switch# clear ospfv3-af ipv4 statistics interface 1/1/1
switch# clear ospfv3-af ipv4 statistics interface 1/1/1 vrf vrf_red
switch# clear ospfv3-af ipv4 statistics interface tunnell
switch# clear ospfv3-af ipv4 statistics interface tunnell vrf vrf_red
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear ospfv3-af ipv6 neighbor

```
clear ospfv3-af [<PROCESS-ID>] ipv6 neighbor [<NEIGHBOR-ID>] [interface <INTERFACE-NAME>
| vlan <VLAN-ID> | lag <LAG-ID> | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>] [all-vrfs
| vrf <VRF-NAME>]
```

Description

Resets the neighbor and clears the OSPFv3 AF neighbor information.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv3 AF process ID to clear the statistics for the particular OSPFv3 AF process. Range: 1 to 65535.
neighbor <NEIGHBOR-ID>	Specifies the router ID of a neighbor.
interface <INTERFACE-NAME>	Specifies the OSPFv3 AF statistics to clear for the specified interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
all-vrfs	Select to clear the OSPFv3 AF statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv3 AF neighbor information:

```
switch# clear ospfv3-af 1 ipv6 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af 1 ipv6 neighbor 3.3.3.3
Performing clear ospf neighbor may result in traffic disruption.
```

```

Do you want to continue (y/n)? y
switch# clear ospfv3-af 1 ipv6 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af 1 ipv6 neighbor 3.3.3.3 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv6 neighbor
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv6 neighbor 5.5.5.5
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv6 neighbor interface 1/1/1
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y
switch# clear ospfv3-af ipv6 neighbor 5.5.5.5 vrf red
Performing clear ospf neighbor may result in traffic disruption.
Do you want to continue (y/n)? y

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear ospfv3-af ipv6 statistics

```

clear ospfv3-af [<PROCESS-ID>] ipv6 statistics [interface [interface <INTERFACE-NAME> |
vlan <VLAN-ID> | lag <LAG-ID>] | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>] [all-vrfs |
vrf <VRF-NAME>]

```

Description

Clears the OSPFv3 AF event statistics.

Parameter	Description
<PROCESS-ID>	Specifies the OSPFv3 AF process ID to clear the statistics for the particular OSPFv3 AF process. Range: 1 to 65535.
interface <INTERFACE-NAME>	Specifies the OSPFv3 AF statistics to clear for the specified interface.

Parameter	Description
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
all-vrfs	Select to clear the OSPFv3 AF statistics for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.

Example

Clearing the OSPFv3 AF event statistics:

```
switch# clear ospfv3-af ipv6 statistics
switch# clear ospfv3-af ipv6 statistics interface 1/1/1
switch# clear ospfv3-af ipv6 statistics interface 1/1/1 vrf vrf_red
switch# clear ospfv3-af ipv6 statistics interface tunnell
switch# clear ospfv3-af ipv6 statistics interface tunnell vrf vrf_red
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

dead-interval

```
dead-interval <INTERVAL>
no dead-interval
```

Description

Sets the interval after which a neighbor is declared dead if no hello packet comes in for virtual links. The **no** form of this command sets the dead interval to default for virtual links. The default value is 40 seconds (generally four times the hello packet interval).



For proper operation, set the dead interval higher than the hello interval.

Parameter	Description
<INTERVAL>	Specifies the time interval for the dead interval, in seconds. Range: 1 to 65535. Default: 40.

Examples

Setting OSPFv3 AF virtual links dead interval:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# dead-interval 30
```

Setting OSPFv3 AF virtual links dead interval to default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

debug ospfv3-af

```
debug ospfv3-af <SUBMODULE-NAME> [instance <PROCESS-ID>] [ip <IP-ADDRESS>] [port <IF-NAME>] [vrf <VRF-NAME>] [severity {alert | crit | debug | emer | err | info | notice | warning}]
no debug ospfv3-af <SUBMODULE-NAME> [instance <PROCESS-ID>] [ip <IP-ADDRESS>] [port <IF-NAME>] [vrf <VRF-NAME>] [severity {alert | crit | debug | emer | err | info | notice | warning}]
```

Description

Enables problem logs to the debug logs. If <SEVERITY> is omitted, all severities are logged.

The **no** form of this command disables problem logs to the debug logs.

Parameter	Description
<code><SUBMODULE-NAME></code>	Enables debug logging for a specific submodule. For a list of supported submodules, enter the debug <code><MODULE-NAME></code> command followed by a space and a question mark (?).
<code>instance <PROCESS-ID></code>	Displays debug logs for the specified OSPFv3 AF process ID. Range: 1 to 65535.
<code>ip <IP-ADDRESS></code>	Displays debug logs for the specified IP Address.
<code>port <INTERFACE-NAME></code>	Displays debug logs for the OSPFv3 AF specified interfaces.
<code>vrf <VRF-NAME></code>	Displays debug logs for the specified VRF name.
<code>severity {alert crit debug emer err info notice warning}</code>	Enables the debug logs for OSPv3 AF based on the required severity level for the destination. Optional.

Examples

Enables debug logging of event submodules for port 1/1/1 and debug severity:

```
switch# debug ospfv3-af ipv4 event port 1/1/1 severity debug
```

Enables all debug logging for VRF red:

```
switch# debug ospfv3-af ipv4 all vrf vrf_red
```

Disables all OSPFv3 AF debug logging:

```
switch# no debug ospfv3-af ipv4 all
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

default-information originate always

```
default-information originate always [metric <METRIC-VALUE>]  
no default-information originate always [metric <METRIC-VALUE>]
```

Description

Configures OSPFv3 AF to advertise the default route (::/0) to its neighbors, regardless if it is present in the routing table or not. Optionally, metric can be set for default route ::/0. The default value is 1. The **no** form of this command disables advertisement of the default route.

Parameter	Description
<i>metric</i> <METRIC-VALUE>	Specifies the OSPF metric value for the default route. Default: 1.

Examples

Setting advertisement of the default route:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv4 unicast  
switch(config-ospfv3-ipv4-uc)# default-information originate always
```

Disabling advertisement of the default route:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv4 unicast  
switch(config-ospfv3-ipv4-uc)# no default-information originate always
```

Setting advertisement of the default route with metric set to 20:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv4 unicast  
switch(config-ospfv3-ipv4-uc)# default-information originate always metric 20
```

Disabling advertisement of the default route and setting the metric to the default value:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv4 unicast  
switch(config-ospfv3-ipv4-uc)# no default-information originate always metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

default-information originate

```
default-information originate [metric <METRIC-VALUE>]
no default-information originate [metric <METRIC-VALUE>]
```

Description

Configures OSPFv3 AF to advertise the default route (::/0) to its neighbors if it is present in the routing table. Optionally, the metric value can be set for default route ::/0. The default value is 1.

The **no** form of this command disables advertisement of the default route.

Parameter	Description
<i>metric</i> <METRIC-VALUE>	Specifies the OSPF metric value for the default route. Optional. Default: 1.

Examples

Setting advertisement of the default route and specifying an optional metric value of 20 :

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# default-information originate
switch(config-ospfv3-ipv4-uc)# default-information originate metric 20
```

Disabling advertisement of the default route:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no default-information originate metric
switch(config-ospfv3-ipv4-uc)# no default-information originate
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

default-metric

```
default-metric <METRIC-VALUE>
no default-metric
```

Description

Sets the default metric for redistributed routes in the OSPFv3 AF.

The **no** form of this command sets the default metric to be used for redistributed routes into OSPFv3 AF to the default of 25.

Parameter	Description
<METRIC-VALUE>	Specifies the default metric value to use for redistributed routes. Range: 1 to 1677214. Default: 25.

Examples

Setting default metric for redistributed routes:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# default-metric 36
```

Setting default metric for redistributed routes to the default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1) # address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc) # no default-metric
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

diag ospfv3 lsdb dump

```
diag ospfv3 lsdb dump
```

Description

This command dumps the OSPFv3 AF protocol LSA information.

Examples

```
switch# diag ospfv3 lsdB dump
ospfv3PmAreaLsdBTable row:
ospfv3PmAreaLsdBApplIndex:      537265152
ospfv3PmAreaLsdBAreaId:        0x00000000
ospfv3PmAreaLsdBType:          ospfv3RouterLsa
ospfv3PmAreaLsdBRouterId:      0x01010103
ospfv3PmAreaLsdBLsid:          0x00000000
ospfv3PmAreaLsdBSequence:      -2147483646
ospfv3PmAreaLsdBAge:           872
ospfv3PmAreaLsdBChecksum:      12468
ospfv3PmAreaLsdBAdvertisement: 0x00 0x01 0x20 0x01 0x00 0x00 0x00 0x00
                                0x01 0x01 0x01 0x03 0x80 0x00 0x00 0x02
                                0x30 0xB4 0x00 0x28 0x01 0x00 0x00 0x13
                                0x02 0x00 0x00 0x01 0x10 0x01 0x01 0x01
                                0x10 0x01 0x01 0x01 0x03 0x03 0x03 0x03
ospfv3PmAreaLsdBTypeKnown:      true

ospfv3PmAreaLsdBTable row:
ospfv3PmAreaLsdBApplIndex:      537265152
ospfv3PmAreaLsdBAreaId:        0x00000000
ospfv3PmAreaLsdBType:          ospfv3RouterLsa
ospfv3PmAreaLsdBRouterId:      0x03030303
ospfv3PmAreaLsdBLsid:          0x00000000
ospfv3PmAreaLsdBSequence:      -2147483646
ospfv3PmAreaLsdBAge:           873
ospfv3PmAreaLsdBChecksum:      64738
ospfv3PmAreaLsdBAdvertisement: 0x00 0x01 0x20 0x01 0x00 0x00 0x00 0x00
                                0x03 0x03 0x03 0x03 0x80 0x00 0x00 0x02
                                0xFC 0xE2 0x00 0x28 0x00 0x00 0x00 0x13
                                0x02 0x00 0x00 0x01 0x10 0x01 0x01 0x01
                                0x10 0x01 0x01 0x01 0x03 0x03 0x03 0x03
ospfv3PmAreaLsdBTypeKnown:      true

ospfv3PmAreaLsdBTable row:
ospfv3PmAreaLsdBApplIndex:      537265152
ospfv3PmAreaLsdBAreaId:        0x00000000
ospfv3PmAreaLsdBType:          ospfv3NetworkLsa
ospfv3PmAreaLsdBRouterId:      0x03030303
ospfv3PmAreaLsdBLsid:          0x10010101
ospfv3PmAreaLsdBSequence:      -2147483647
ospfv3PmAreaLsdBAge:           878
ospfv3PmAreaLsdBChecksum:      45127
ospfv3PmAreaLsdBAdvertisement: 0x00 0x01 0x20 0x02 0x10 0x01 0x01 0x01
                                0x03 0x03 0x03 0x03 0x80 0x00 0x00 0x01
                                0xB0 0x47 0x00 0x20 0x00 0x00 0x00 0x13
                                0x01 0x01 0x01 0x03 0x03 0x03 0x03 0x03
ospfv3PmAreaLsdBTypeKnown:      true

ospfv3PmAreaLsdBTable row:
ospfv3PmAreaLsdBApplIndex:      537265152
ospfv3PmAreaLsdBAreaId:        0x00000000
ospfv3PmAreaLsdBType:          ospfv3InterAreaPrfxLsa
ospfv3PmAreaLsdBRouterId:      0x01010103
ospfv3PmAreaLsdBLsid:          0x00000001
ospfv3PmAreaLsdBSequence:      -2147483647
ospfv3PmAreaLsdBAge:           913
ospfv3PmAreaLsdBChecksum:      13755
ospfv3PmAreaLsdBAdvertisement: 0x00 0x24 0x20 0x03 0x00 0x00 0x00 0x01
                                0x01 0x01 0x01 0x03 0x80 0x00 0x00 0x01
                                0x35 0xBB 0x00 0x24 0x00 0x00 0x00 0x01
                                0x40 0x00 0x00 0x00 0xFD 0x00 0x00 0x00
```

```

ospfv3PmAreaLsdbTypeKnown:      0x00 0x00 0x00 0x00
                                true

ospfv3PmAreaLsdbTable row:
ospfv3PmAreaLsdbApplIndex:      537265152
ospfv3PmAreaLsdbAreaId:         0x00000000
ospfv3PmAreaLsdbType:           ospfv3IntraAreaPrfxLsa
ospfv3PmAreaLsdbRouterId:       0x03030303
ospfv3PmAreaLsdbLsid:           0x00010000
ospfv3PmAreaLsdbSequence:       -2147483645
ospfv3PmAreaLsdbAge:            873
ospfv3PmAreaLsdbChecksum:       2173
ospfv3PmAreaLsdbAdvertisement:   0x00 0x01 0x20 0x09 0x00 0x01 0x00 0x00
                                0x03 0x03 0x03 0x03 0x80 0x00 0x00 0x03
                                0x08 0x7D 0x00 0x2C 0x00 0x01 0x20 0x02
                                0x10 0x01 0x01 0x01 0x03 0x03 0x03 0x03
                                0x40 0x00 0x00 0x00 0x01 0x11 0x00 0x00
                                0x00 0x00 0x00 0x00

ospfv3PmAreaLsdbTypeKnown:      true

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables the OSPFv3 AF process. By default OSPFv3 AF process is enabled.

This command does not remove the OSPFv3 AF configurations.



The configuration is supported globally as well as per address-families ipv4-unicast or ipv6-unicast. If address-family specific timers is configured, it takes precedence over global configuration.

Example

Disabling OSPFv3 AF process:

```
switch(config)# router ospfv3-af 1
```



```
switch(config-ospfv3-af-1) # disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

distance

```
distance [<DISTANCE-VAL> | intra-area [<DISTANCE-VAL>] | inter-area [<DISTANCE-VAL>] |  
external [<DISTANCE-VAL>]]  
no distance [<DISTANCE-VAL> | intra-area [<DISTANCE-VAL>] | inter-area [<DISTANCE-VAL>] |  
external [<DISTANCE-VAL>]]
```

Description

Defines an administrative distance for OSPFv3 AF. Administrative distance is used as a criteria to select the best route when the same route is learned by multiple routing protocols.

The **no** form of this command sets the OSPFv3 AF administrative distance to the default value of 110. Optionally, administrative distance can be set to default for the specific OSPF route type: intra-area, inter-area, or external type-5 and type-7 routes.

Parameter	Description
<DISTANCE-VAL>	Specifies the OSPFv3 AF administrative distance. Range: 1 to 255. Default: 110.
intra-area	Specifies the OSPFv3 AF distance for intra-area routes.
inter-area	Specifies the OSPFv3 AF distance for inter-area routes.
external	Specifies the OSPFv3 AF distance for external type 5 and type 7 routes.

Usage

Within a given OSPF process, intra-area routes are always given precedence even when distances are configured for inter-area or external type routes.

Examples

Setting OSPFv3 AF administrative distance for address-family ipv6-unicast:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# distance 100
switch(config-ospfv3-ipv6-uc)# distance intra-area 24 external 55 inter-area 66
switch(config-ospfv3-ipv6-uc)# distance intra-area 24 external 55
switch(config-ospfv3-ipv6-uc)# distance external 55
switch(config-ospfv3-ipv6-uc)#exit
```

Setting OSPFv3 AF administrative distance for address-family ipv4-unicast to default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no distance
switch(config-ospfv3-ipv4-uc)# no distance external
switch(config-ospfv3-ipv4-uc)# no distance intra-area
switch(config-ospfv3-ipv4-uc)# no distance inter-area
switch(config-ospfv3-ipv4-uc)# no distance 1
switch(config-ospfv3-ipv4-uc)#exit
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

distribute-list prefix

```
distribute-list prefix <PREFIX-LIST-NAME> {in | out}
no distribute-list prefix <PREFIX-LIST-NAME> {in | out}
```

Description

This command uses an existing prefix list to filter routes that are being installed in the routing table or redistributed to another routing protocol.

The **distribute-list prefix** command filters routes in the inbound or the outbound direction. When this command is issued with the **in** parameter, it filters routes from being installed in the routing table, it does not filter LSAs. When this command is issued with the **out** parameter, it filters only the desired redistributed routes from other protocols.

Parameter	Description
<code>prefix <PREFIX-LIST-NAME></code>	Specify the name of an existing prefix.
<code>{in out}</code>	Select one of the following parameters to set the filter direction: ▪ in: Filter incoming routes into the routing table ▪ out: Filter outgoing routing updates

Examples

Enabling the filtering of OSPFv3 AF routes for an IPv4 network, preventing routes from being installed in the routing table or redistributed from another routing protocol.

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# distribute-list prefix list1 in
switch(config-ospfv3-ipv4-uc)# distribute-list prefix list2 out
```

Disabling the filtering of OSPFv3 AF routes for an IPv4 network, allowing routes to be installed in the routing table or redistributed from another routing protocol.

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no distribute-list prefix list1 in
switch(config-ospfv3-ipv4-uc)# no distribute-list prefix list2 out
```

Enabling the filtering of OSPFv3 AF routes for an IPv6 network, preventing routes from being installed in the routing table or redistributed from another routing protocol.

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# distribute-list prefix list1 in
switch(config-ospfv3-ipv6-uc)# distribute-list prefix list2 out
```

Disabling the filtering of OSPFv3 AF routes for an IPv6 network, allowing routes to be installed in the routing table or redistributed from another routing protocol.

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# no distribute-list prefix list1 in
switch(config-ospfv3-ipv6-uc)# no distribute-list prefix list2 out
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

enable

enable

Description

Enables OSPFv3 AF process when disabled. By default OSPFv3 AF process is enabled.



Configuration is supported both globally and in the address-family for ipv4-unicast and ipv6-unicast. If enable is configured for the address-family, it will override the global configuration.

Example

Enabling OSPFv3 AF process:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-af-<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S		

encryption ipsec

```
encryption ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>
{<ENCR-TYPE> [<KEY-TYPE> <ENCR-KEY>] | null}]
no encryption
```

Description

Configures IPsec ESP authentication and encryption for the selected Vlink.

The **no** form of this command removes IPsec ESP authentication and encryption for the selected Vlink.

Parameter	Description
<code>spi <SPI-INDEX></code>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPFv3 AF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<code><AUTH-TYPE></code>	Specifies the authentication type: md5 or sha1 .
<code><KEY-TYPE></code>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<code><AUTH-KEY></code>	Specifies the authentication key.
<code><ENCR-TYPE></code>	Specifies the encryption type: des , 3des , aes , or null . NOTE: Encryption type aes is considered to be AES128, AES192, or AES256 based on key length.
<code><ENCR-KEY></code>	Specifies the encryption key.



When the authentication key is not provided on the command line, plaintext authentication key prompting occurs upon pressing Enter, followed by encryption type prompting, and finally plaintext encryption key prompting. The entered key characters are masked with asterisks.



When the authentication key and encryption type are provided on the command line but the encryption key is not provided, plaintext encryption key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting area 1 to use IPsec ESP authentication and encryption for Vlink with provided plaintext keys:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5 plaintext abcd
                                des plaintext abcdefab
```

Setting area 1 to use IPsec md5 authentication and encryption for Vlink with a prompted plaintext authentication key and encryption type:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? des
```

```
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting area 1 to use IPsec sha1 authentication and encryption for Vlink with a provided plaintext authentication key and prompted encryption type:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 sha1 plaintext pass des
    ciphertext    Configure ciphertext key.
    hex-string    Configure hex-string key. Key length must be 16 Hex digits.
    plaintext     Configure plaintext key. Key length must be 8 characters.

switch(config-router-vlink6)# encryption ipsec spi 256 sha1 plaintext pass des
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting area 1 to use IPsec ESP authentication for Vlink with a provided plaintext authentication key and null encryption:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-1)# area 1
switch(config-ospfv3-1)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# encryption ipsec spi 256 md5 plaintext abcd null
```

Removing IPsec ESP authentication and encryption for Vlink on area 1:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 1 virtual-link 3.3.3.3
switch(config-router-vlink6)# no encryption
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

graceful-restart ignore-lost-interface

```
graceful-restart ignore-lost-interface
no graceful-restart ignore-lost-interface
```

Description

Enables the restarting router to ignore lost OSPFv3 AF interfaces during a graceful restart process. It is recommended to enable the ignore-lost-interface parameter on the VSF device configured with OSPF enabled on ROPs to ensure the graceful restart completes successfully, as a VSF switchover or failover can render a ROP non-operational, leading to a Router LSA change published to neighbors.

The **no** form of this commands disables the restarting router to ignore OSPFv3 AF interfaces during a graceful restart process.



Configuration is supported both globally and in the address-family for ipv4-unicast and ipv6-unicast. If disable is configured for the address-family, it will override the global configuration.

Parameter	Description
ignore-lost-interface	Enable the restarting router to ignore lost OSPFv3 AF interfaces during a graceful restart process. This setting should be enabled on a high availability system to ensure a graceful restart completes successfully, even if OSPFv3 AF-enabled links fail due to High Availability events like a switchover or failover. NOTE: Enabling this setting means that the hitless restart procedures do not strictly follow those defined in <i>RFC 3623, Graceful OSPF Restart</i>. NOTE: OSPFv3 AF neighbors must disable strict LSA checking. If the local node has fewer OSPFv3 AF interfaces after restarting, then the neighbors that were adjacent on those interfaces will clear up their adjacencies to the restarting node and will send out link state updates to advertise the dropped adjacency. If strict LSA checking is enabled, the restarting router's neighbors will exit helper mode when they receive the updated LSAs and the graceful restart will still fail.

Examples

Enabling the restarting router to ignore lost OSPFv3 AF interfaces during a graceful restart process:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv4-uc) # graceful-restart ignore-lost-interface
```

Disabling the restarting router:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv4-uc) # no graceful-restart ignore-lost-interface
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

graceful-restart

```
graceful-restart {restart-interval <INTERVAL> | helper [strict-lsa-check]}  
no graceful-restart {restart-interval <INTERVAL> | helper [strict-lsa-check]}
```

Description

Configures graceful restart for OSPFv3 AF. By default graceful restart is enabled on the OSPFv3 AF router.

The **no** form of this command sets the restart interval to the default of 120 seconds or disables helper mode depending on the specified parameters.



Configuration is supported both globally and in the address-family for ipv4-unicast and ipv6-unicast. If disable is configured for the address-family, it will override the global configuration.

Parameter	Description
restart-interval <INTERVAL>	Specifies the time another router waits for this router to gracefully restart and selects the maximum time to wait in seconds. Range: 5 to 1800. Default: 120.
helper	Specifies that the router will participate in the graceful restart of a neighbor router.
strict-lsa-check	(Optional). Use with the helper parameter to enable strict Link state Advertisement (LSA) checking when acting as a restart helper for a restarting peer. NOTE: If strict LSA checking is enabled, the restarting router's neighbors will exit helper mode when they receive the updated LSAs and the graceful restart will still fail.

Examples

Enabling OSPFv3 AF graceful restart:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-ipv4-uc)# graceful-restart helper  
switch(config-ospfv3-ipv4-uc)# graceful-restart helper strict-lsa-check
```



```
switch(config-ospfv3-ipv4-uc) # graceful-restart restart-interval 40
```

Setting the restart interval to default, and disabling helper mode:

```
switch(config) # router ospfv3-af 1
switch(config-ospfv3-ipv4-uc) # no graceful-restart
switch(config-ospfv3-ipv4-uc) # no graceful-restart helper
switch(config-ospfv3-ipv4-uc) # no graceful-restart helper strict-lsa-check
switch(config-ospfv3-ipv4-uc) # no graceful-restart restart-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

hello-interval

```
hello-interval <INTERVAL>
no hello-interval
```

Description

Sets the time interval between OSPFv3 AF hello packets for virtual links.

The **no** form of this command sets the hello interval to the default value of 10 seconds for virtual links.



For proper operation, set the hello interval lower than the dead interval.

Parameter	Description
<INTERVAL>	Specifies the time interval for the hello interval, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting OSPFv3 AF virtual links hello interval:

```
switch(config) # router ospfv3-af 1
switch(config-ospfv3-af-1) # address-family ipv6 unicast
```

```
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink6)# hello-interval 30
```

Setting OSPFv3 AF virtual links hello interval to default:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv6 unicast  
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1  
switch(config-router-vlink6)# no hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 retransmit-interval

```
ospfv3-af ipv4 retransmit-interval <INTERVAL>  
no ospfv3-af ipv4 retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for the OSPFv3 AF interface.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default of 5 seconds for the OSPFv3 AF interface.

Parameter	Description
<INTERVAL>	Specifies the retransmit interval, in seconds. Range: 1 to 3600. Default: 5.

Examples

Setting OSPFv3 AF retransmit interval on the interface:

```
switch(config)# interface 1  
switch(config-if)# ospfv3-af ipv4 retransmit-interval 30
```

Setting OSPFv3 AF retransmit interval to the default on the interface:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv4 retransmit-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 cost

```
ospfv3-af ipv4 cost <INTERFACE-COST>
no ospfv3-af ipv4 cost
```

Description

Sets the cost (metric) associated with a particular interface. The interface cost is used as a parameter to calculate the best routes.

The **no** form of this command sets the cost (metric) associated with a particular interface to the default of 1. The default cost is calculated automatically depending on the bandwidth of the interface.

Parameter	Description
<INTERFACE-COST>	Specifies the interface cost value. Range: 1 to 65535. Default: 1.

Examples

Setting OSPFv3 AF interface cost:

```
switch(config)# interface 1
switch(config-if)# ospfv3-af ipv4 cost 100
```

Setting the OSPFv3 AF interface cost to default:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv4 cost
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 hello-interval

```
ospfv3-af ipv4 hello-interval <INTERVAL>  
no ospfv3-af ipv4 hello-interval
```

Description

Sets the time interval between OSPFv3 AF hello packets for the OSPFv3 AF interface.

The **no** form of this command sets the time interval between OSPFv3 AF hello packets to the default for the OSPFv3 AF interface of 10 seconds.



For proper operation, set the hello interval lower than the dead interval.

Parameter	Description
<INTERVAL>	Specifies the time interval between hello packets, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting OSPFv3 AF hello interval on the interface:

```
switch(config)# interface 1/1/1  
switch(config-if)# ospfv3-af ipv4 hello-interval 30
```

Setting OSPFv3 AF hello interval to default on the interface:

```
switch(config)# interface 1/1/1  
switch(config-if)# no ospfv3-af ipv4 hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 network

```
ospfv3-af ipv4 network {broadcast|point-to-point}
no ospfv3-af ipv4 network {broadcast|point-to-point}
```

Description

Configures the network type for the interface. By default the network type is broadcast network. The **no** form of this command sets the network type for the interface to the system default as broadcast network for ethernet interface and point-to-point network for tunnel interface.

Parameter	Description
broadcast	Specifies the OSPFv3 AF network type as a broadcast multiaccess network.
point-to-point	Specifies the OSPFv3 AF network type as a point-to-point network.

Examples

Setting OSPFv3 AF network type for the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv4 network broadcast
switch(config-if)# ospfv3-af ipv4 network point-to-point
```

Disabling OSPFv3 AF network type for the interface to system default of broadcast network:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af ipv4 network
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 priority

```
ospfv3-af ipv4 priority <number-value>
no ospfv3-af ipv4 priority
```

Description

Sets the OSPFv3 AF priority for the interface. The larger the numeric value of the priority, the higher the chance it will become the designated router. Setting a priority of 0 makes the router ineligible to become a designated router or back up designated router.

The **no** form of this command sets the OSPFv3 AF priority for the interface to the default of 1.

Parameter	Description
<number-value>	Specifies the priority value. Default: 1. Range: 0 to 255.

Examples

Setting the OSPFv3 AF priority for the interface:

```
switch(config)# interface 1
switch(config-if)# ospfv3-af ipv4 priority 50
```

Setting the OSPFv3 AF priority for the interface to the default of 1:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv4 priority
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 shutdown

```
ospfv3-af ipv4 shutdown
no ospfv3-af ipv4 shutdown
```

Description

Disables OSPFv3 AF on the interface. The interface state changes to Down. It does not remove the interface from the OSPF area. To remove the interface, use the command **no ospfv3-af ipv4 area**. The **no** form of this command re-enables OSPFv3 AF on the interface.

Examples

Disabling OSPFv3 AF on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv4 shutdown
```

Re-enabling OSPFv3 AF on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af ipv4 shutdown
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 transit-delay

```
ospfv3-af ipv4 transit-delay <seconds>
no ospfv3-af ipv4 transit-delay <seconds>
```

Description

Sets the time delay in Link state transmission for the OSPFv3 AF interface.

The **no** form of this command sets the transit delay in Link state transmission to the default of 1 second.

Parameter	Description
<DELAY>	Specifies the time delay for the transit delay, in seconds. Range: 1 to 3600. Default: 1.

Parameter	Description
<i>no</i>	Sets the delay in Link state transmission to the default of 1 for virtual links.

Examples

Setting OSPFv3 AF transit delay on the interface

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv4 transit-delay 30
```

Setting OSPFv3 AF transit delay to default on the interface

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af ipv4 transit-delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 area

```
ospfv3-af <PROCESS-ID> ipv6 area <AREA-ID>
no ospfv3-af <PROCESS-ID> ipv6 area <area-id>
```

Description

This command runs the OSPFv3 AF IPv6 on the interface with the configured link-local IPv6 address for the area specified. To move an interface to a new area, unmap the existing area and then associate a new area with the interface. If the OSPFv3 AF process or area is not created, user confirmation is requested to create the OSPFv3 AF process and area.

The **no** form of this command disables OSPFv3 AF on the interface and removes the interface from the area. Interfaces which have an IP address configured on the network or in a subset of the network, stop participating in the OSPF protocol

Parameter	Description
<AREA-ID>	Specifies the area ID is one of the following formats. Area ID in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Area ID as a decimal value. Range: 0-4294967295.
<PROCESS-ID>	Specifies the OSPFv3 AF process ID. Range: 1 to 65535.

Examples

Setting OSPFv3 AF network for the area:

```
switch(config)# interface 1
switch(config-if)# ospfv3-af 1 ipv6 area 1
switch(config-if)# ospfv3-af 1 ipv6 area 0.0.0.1
```

Disabling OSPFv3 AF network for the area:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af 1 ipv6 area 1
switch(config-if)# no ospfv3-af 1 ipv6 area 0.0.0.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 cost

```
ospfv3-af ipv6 cost <INTERFACE-COST>
no ospfv3-af ipv6 cost
```

Description

Sets the cost (metric) associated with a particular interface. The interface cost is used as a parameter to calculate the best routes.

The **no** form of this command sets the cost (metric) associated with a particular interface to the default which is calculated automatically depending on the bandwidth of the interface.

Parameter	Description
<code><INTERFACE-COST></code>	Specifies the interface cost value. Range: 1 to 65535. Default: 1.

Examples

Setting OSPFv3 AF interface cost:

```
switch(config)# interface vlan 1
switch(config-if)# ospfv3-af ipv6 cost 20
```

Setting the OSPFv3 AF interface cost to default:

```
switch(config)# interface vlan 1
switch(config-if)# no ospfv3-af ipv6 cost
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 dead-interval

```
ospfv3-af ipv6 dead-interval <seconds>
no ospfv3-af ipv6 dead-interval
```

Description

Sets the interval after a neighbor is declared dead when no hello packet is received on the OSPFv3 AF interface. Dead interval must be greater than hello interval, otherwise, the OSPF protocol will have an undefined behavior.

The **no** form of this command sets the interval after which a neighbor is declared dead, to the default for the OSPFv3 AF interface. The default value is 40 seconds (generally four times the hello packet interval).

Parameter	Description
<code><seconds></code>	Specifies the time interval for the dead interval, in seconds. Range: 1 to 65535. Default: 40.

Examples

Setting OSPFv3 AF dead interval on the interface:

```
switch(config)# interface 1
switch(config-if)# ospfv3-af ipv6 dead-interval 30
```

Setting OSPFv3 AF dead interval to default on the interface:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv6 dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 hello-interval

```
ospfv3-af ipv6 hello-interval <INTERVAL>
no ospfv3-af ipv6 hello-interval
```

Description

Sets the time interval between OSPFv3 AF hello packets for the OSPFv3 AF interface.

The **no** form of this command sets the time interval between OSPFv3 AF hello packets to the default for the OSPFv3 AF interface of 10 seconds.



For proper operation, set the hello interval lower than the dead interval.

Parameter	Description
<INTERVAL>	Specifies the time interval between hello packets, in seconds. Range: 1 to 65535. Default: 10.

Examples

Setting OSPFv3 AF hello interval on the interface:

```
switch(config)# interface 1
switch(config-if)# ospfv3-af ipv6 hello-interval 30
```

Setting OSPFv3 AF hello interval to default on the interface:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv6 hello-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 network

```
ospfv3-af ipv6 network {broadcast|point-to-point}
no ospfv3-af ipv6 network {broadcast|point-to-point}
```

Description

Configures the network type for the interface. By default the network type is broadcast network.

The **no** form of this command sets the network type for the interface to the system default as broadcast network for ethernet interface and point-to-point network for tunnel interface.

Parameter	Description
broadcast	Specifies the OSPFv3 AF network type as a broadcast multiaccess network.
point-to-point	Specifies the OSPFv3 AF network type as a point-to-point network.

Examples

Setting OSPFv3 AF network type for the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv6 network broadcast
switch(config-if)# ospfv3-af ipv6 network point-to-point
```

Disabling OSPFv3 AF network type for the interface to system default of broadcast network:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af ipv6 network
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 passive

```
ospfv3-af ipv6 passive
no ospfv3-af ipv6 passive
```

Description

Configures the interface as an OSPFv3 AF passive interface. With this setting, the interface participates in the OSPF, but does not send or receive OSPF packets on that interface.

The **no** form of this command resets the interface as active. With this setting, the interface starts sending and receiving OSPF packets.

Examples

Setting the interface as OSPFv3 AF passive interface:

```
switch(config)# interface vlan 1
switch(config-if)# ospfv3-af ipv6 passive
```

Setting the interface as OSPFv3 AF active interface:

```
switch(config)# interface vlan 1
switch(config-if)# no ospfv3-af ipv6 passive
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 priority

```
ospfv3-af ipv6 priority <number-value>
no ospfv3-af ipv6 priority
```

Description

Sets the OSPFv3 AF priority for the interface. The larger the numeric value of the priority, the higher the chance it will become the designated router. Setting a priority of 0 makes the router ineligible to become a designated router or back up designated router.

The **no** form of this command sets the OSPFv3 AF priority for the interface to the default of 1.

Parameter	Description
<number-value>	Specifies the OSPFv3 AF priority value. Default: 1. Range: 0 to 255.

Examples

Setting the OSPFv3 AF priority for the interface:

```
switch(config)# interface vlan /1
switch(config-if)# ospfv3-af ipv6 priority 50
```

Setting the OSPFv3 AF priority for the interface to the default of 1:

```
switch(config)# interface vlan 1
switch(config-if)# no ospfv3-af ipv6 priority
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 retransmit-interval

```
ospfv3-af ipv6 retransmit-interval <INTERVAL>
no ospfv3-af ipv6 retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for the OSPFv3 AF interface.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default 5 seconds.

Parameter	Description
<INTERVAL>	Specifies the time interval for the retransmit interval, in seconds. Range: 1 to 3600. Default: 5

Examples

Setting OSPFv3 AF retransmit interval on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv6 retransmit-interval 30
```

Setting OSPFv3 AF retransmit interval to the default on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af ipv6 retransmit-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 shutdown

```
ospfv3-af ipv6 shutdown
no ospfv3-af ipv6 shutdown
```

Description

Disables OSPFv3 AF on the interface. The interface state changes to Down. It does not remove the interface from the OSPF area. To remove the interface, use the command **no ospfv3-af ipv6 area**. The **no** form of this command re-enables OSPFv3 AF on the interface.

Examples

Disabling OSPFv3 AF on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv6 shutdown
```

Re-enabling OSPFv3 AF on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af ipv6 shutdown
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv6 transit-delay

```
ospfv3-af ipv6 transit-delay <seconds>
no ospfv3-af ipv6 transit-delay <seconds>
```

Description

Sets the time delay in Link state transmission for the OSPFv3 AF virtual link.

The **no** form of this command sets the transit delay in Link state transmission to the default of 1 second.

Parameter	Description
<DELAY>	Specifies the time delay for the transit delay, in seconds. Range: 1

Parameter	Description
	to 3600. Default: 1.
<i>no</i>	Sets the delay in Link state transmission to the default of 1 for virtual links.

Examples

Setting OSPFv3 AF transit delay on the interface

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# transit-delay 30
```

Setting OSPFv3 AF transit delay to default on the interface

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no transit-delay
switch(config-router-vlink6)# no transit-delay 30
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

max-metric router-lsa

```
max-metric router-lsa [include-stub] | [on-startup <INTERVAL>]
no max-metric router-lsa [include-stub] | [on-startup]
```

Description

Sets the protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations. If the on-startup parameter is used, the router is configured to advertise a maximum metric at start up. That is, for the time specified in seconds, or the default value of 600 seconds. The include-stub parameter configures the router to advertise maximum metric for links including stub links.

To disable advertisement of the maximum metric, use the **no** form of the command.

The **no** form of this command advertises the normal cost metrics instead of advertising the maximized cost metric. This setting causes the router to be considered in traffic forwarding.

Parameter	Description
<code>on-startup</code> <code><INTERVAL></code>	Automatically advertises the stub Router-LSA (or maximize the router-LSA cost metric) for a specified time interval upon OSPFv3 AF startup. Specifies the time in seconds. Range: 5 to 86400. Default: 600.
<code>include-stub</code>	Advertise router-LSAs with maximum metric value for stub links.

Examples

Setting to maximize the cost metrics for Router LSA:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# address-family ipv6 unicast  
switch(config-ospfv3-ipv6-uc)# max-metric router-lsa on-startup 3000
```

Setting to advertise the normal cost metrics instead of advertising the maximized cost metric:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# no max-metric router-lsa  
switch(config-ospfv3-ipv6-uc)# no max-metric router-lsa on-startup
```

Setting to advertise Router LSA for stub links:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# max-metric router-lsa  
switch(config-ospfv3-ipv6-uc)# max-metric router-lsa include-stub on-startup 3000
```

Setting to advertise the normal cost metrics instead of advertising the maximized cost metric for stub links:

```
switch(config)# router ospfv3 1  
switch(config-ospfv3-af-1)# no max-metric router-lsa  
switch(config-ospfv3-ipv6-uc)# no max-metric router-lsa include-stub on-startup
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

maximum-paths

```
maximum-paths <MAXIMUM>
no maximum-paths
```

Description

Sets the maximum number of ECMP routes that OSPFv3 AF can support.

The **no** form of this command sets the maximum number of ECMP routes that OSPFv3 AF can support to the default value of 4.

Parameter	Description
<MAXIMUM>	Specifies the maximum number of ECMP routes. Range: 1 to 32. Default: 4.

Examples

Setting maximum number of parallel routes:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)#address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# maximum-paths 3
```

Setting maximum number of parallel paths to the default value of 4:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)#address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc)# no maximum-paths
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

OSPFv3 AF commands

ospfv3-af encryption ipsec spi

```
ospfv3-af encryption ipsec spi <SPI-INDEX> <AUTH-TYPE>
    [<KEY-TYPE> <AUTH-KEY> <ENCR-TYPE> [<KEY-TYPE> <ENCR-KEY>]]
no ospfv3-af encryption {null| [ipsec spi <SPI-INDEX> <AUTH-TYPE>
    [<KEY-TYPE><AUTH-KEY><ENCR-TYPE> [<KEY-TYPE><ENCR-KEY>]] }
```

Description

Configures IPsec ESP authentication. OSPFv3 interfaces that have IPsec configured at the interface context will not use area level IPsec ESP.

The **no** form of this command removes IPsec ESP for the specified area.

Parameter	Description
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.
<ENCR-TYPE>	Specifies the encryption type: des , 3des , aes , or null . NOTE: Encryption type aes is considered to be AES128, AES192, or AES256 based on key length.
<ENCR-KEY>	Specifies the encryption key.



When the authentication key is not provided on the command line, plaintext authentication key prompting occurs upon pressing Enter, followed by encryption type prompting, and finally plaintext encryption key prompting. The entered key characters are masked with asterisks.



When the authentication key and encryption type are provided on the command line but the encryption key is not provided, plaintext encryption key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting interface VLAN 1 to use IPsec ESP with provided authentication and encryption keys:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ospfv3-af encryption ipsec spi 256 sha1 plaintext F82
```

```
des plaintext F82#450b
```

Setting interface VLAN 3 to use IPsec ESP with prompted authentication and encryption keys:

```
switch(config)# interface vlan 3
switch(config-if-vlan)# ospfv3-af encryption ipsec spi 256 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? des

Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting interface VLAN 4 to use IPsec ESP with provided authentication password and encryption type but a prompted encryption key:

```
switch(config)# interface vlan 4
switch(config-if-vlan)# ospfv3-af encryption ipsec spi 256 sha1 plaintext F82 des
Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting interface VLAN 1 to use IPsec ESP with provided plaintext authentication key and null encryption:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# ospfv3-af encryption ipsec spi 256 sha1 plaintext F82 null
```

Removing IPsec from interface VLAN 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no ospfv3-af encryption ipsec spi
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af authentication ipsec spi

```
ospfv3-af authentication ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY>]
no ospfv3-af authentication ipsec spi
```

Description

Configures IPsec AH authentication. OSPFv3 AF interfaces that have IPsec configured at the interface context will not use area level IPsec. The Security Parameters Index (SPI) is an identification tag carried in IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table.

The **no** form of this command removes IPsec AH authentication for the specified area.



IPsec is not supported for 6in6 tunnel interfaces, and IPsec AH SPI must be unique on the router.

Parameter	Description
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.



When the authentication key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting interface **1/1/1** to use IPsec authentication with a provided plaintext authentication key:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af authentication ipsec spi 256 md5 plaintext abcd
```

Setting interface **1/1/1** to use IPsec authentication with a prompted plaintext authentication key:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af authentication ipsec spi 256 md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Removing IPsec authentication from interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af authentication
switch(config-if)# no ospfv3-af authentication null
switch(config-if)# no ospfv3-af authentication ipsec spi 300 md5 ciphertext
```

```
qwertyuioplkjhgfdsxcvbnm
switch(config-if)# no ospfv3-af authentication ipsec spi 300 sha1 ciphertext
qwertyuioplkjhgfdsxcvbnm
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af encryption ipsec

```
ospfv3-af encryption ipsec spi <SPI-INDEX> <AUTH-TYPE> [<KEY-TYPE> <AUTH-KEY> {<ENCR-
TYPE> [<KEY-TYPE> <ENCR-KEY>] | null}]
no ospfv3-af encryption {null | [ipsec spi <SPI-INDEX> <AUTH-TYPE> ciphertext <AUTH-KEY>
[<ENCR-TYPE> ciphertext <ENCR-KEY>] | null]}
```

Description

Configures IPsec ESP authentication. OSPFv3 AF interfaces that have IPsec configured at the interface context will not use area level IPsec ESP.

The **no** form of this command removes IPsec ESP for the specified area.



IPsec is not supported in 6in6 tunnel interfaces.

Parameter	Description
spi <SPI-INDEX>	Specifies the Security Parameters Index (SPI) to use. The SPI is an identification tag carried in the IPsec AH header. It enables the receiving OSPF process to select and use the Security Association (SA) from the SA table. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication type: md5 or sha1 .
<KEY-TYPE>	Specifies the key type to use: plaintext (unencrypted), hex-string (encrypted) or ciphertext (encrypted).
<AUTH-KEY>	Specifies the authentication key.
<ENCR-TYPE>	Specifies the encryption type: des , 3des , aes , or null .

Parameter	Description
	NOTE: Encryption type aes is considered to be AES128, AES192, or AES256 based on key length.
<ENCR-KEY>	Specifies the encryption key.



When the authentication key is not provided on the command line, **plaintext** authentication key prompting occurs upon pressing Enter, followed by encryption type prompting, and finally **plaintext** encryption key prompting. The entered key characters are masked with asterisks.



When the authentication key and encryption type are provided on the command line but the encryption key is not provided, **plaintext** encryption key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

Examples

Setting interface **1/1/1** to use IPsec ESP with provided authentication and encryption keys:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af encryption ipsec spi 256 sha1 plaintext abcdef
aes plaintext abcdefabcdefabcdefab
```

Setting interface **1/1/1** to use IPsec ESP with provided plaintext authentication key and null encryption:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af encryption ipsec spi 256 sha1 plaintext abcdef null
```

Setting interface **1/1/1** to use IPsec ESP with prompted authentication and encryption keys:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af encryption ipsec spi 256 sha1
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****

Enter the IPsec encryption type (3des/aes/des/null)? des

Enter the IPsec encryption key: *****
Re-Enter the IPsec encryption key: *****
```

Setting interface **1/1/1** to use IPsec ESP with provided authentication password and encryption type but a prompted encryption key:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af encryption ipsec spi 256 sha1 plaintext abcdef des
ciphertext    Configure ciphertext key.
hex-string    Configure hex-string key. Key length must be 16 Hex digits.
plaintext     Configure plaintext key. Key length must be 8 characters.
Enter the IPsec encryption key: *****
```


Re-Enter the IPsec encryption key: *****

Removing IPsec from interface **1/1/1**:

```
switch(config) # interface 1/1/1  
switch(config-if) # no ospfv3-af encryption
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 area

```
ospfv3-af <process-id> ipv4 area <area-id>  
no ospfv3-af <process-id> ipv4 area <area-id>
```

Description

This command will run the OSPFv3 AF protocol on the interface with the configured link-local IPv6 address for the area mentioned. For moving an interface to a new area, you need to unmap the existing area and then associate a new area to the interface. If the OSPFv3 AF process or area is not created, user confirmation is requested to create the OSPFv3 AF process and area.

The **no** form of this command disables OSPFv3 AF on the interface.



An IPv6 link-local address must be enabled on the interface for an OSPFv3 AF adjacency to be formed for the IPv4 unicast OSPFv3 AF.

Parameter	Description
<process-id>	Specify the OSPFv3 AF Process ID. Range: 1-65535
area-id	Area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255 or using a decimal value (0-4294967295).

Examples

Enabling OSPFv3 AF on an interface using IPv4 address:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af 1 ipv4 area 1
switch(config-if)# ospfv3-af 1 ipv4 area 0.0.0.1
```

Disabling OSPFv3 AF on an interface using IPv4 address:

```
switch(config)# interface 1/1/1
switch(config-if)# no ospfv3-af 1 ipv4 area 1
switch(config-if)# no ospfv3-af 1 ipv4 area 0.0.0.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af ipv4 dead-interval

ospfv3-af ipv4 dead-interval <seconds>

Description

This command sets the interval after which a neighbor is declared dead if no hello packet is received for the OSPFv3 AF interface. Dead interval must always be greater than hello-interval, otherwise the OSPFv3 AF protocol will have undefined behavior.

The **no** form of this command sets the interval to the default value of 40 seconds.

Parameter	Description
<i>seconds</i>	Specifies Dead interval value in second. Default is 40. Range: 1-65535

Examples

Configuring an interval of 30 to consider an unresponsive neighbor as down:

```
switch(config)# interface 1
switch(config-if)# ospfv3-af ipv4 dead-interval 30
```

Setting the dead interval to the default value:

```
switch(config)# interface 1
switch(config-if)# no ospfv3-af ipv4 dead-interval
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ospfv3-af authentication null

ospfv3-af authentication null

Description

This command configures NULL authentication on an interface which disables IPsec AH authentication.



Ipsec is not supported on 6in6 Tunnel Interfaces.

Examples

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af authentication null
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

ospfv3-af encryption null

ospfv3-af encryption null

Description

This command configures NULL ESP on an interface, which disables IPsec ESP.



IPsec is not supported on 6in6 Tunnel Interfaces.

Example

Configuring null ESP:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af encryption null
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ospfv3-af ipv4 passive

ospfv3-af ipv4 passive

Description

This command configures the interface as an OSPFv3 AF passive interface. With this setting the interface participates in OSPF but does not receive or send OSPF packets on that interface.

Example

Configuring interface 1/1/1 as an OSPFv3 AF passive interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ospfv3-af ipv4 passive
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

passive-interface default

```
passive-interface default  
no passive-interface default
```

Description

Sets all OSPFv3 AF interfaces as passive.

The **no** form of this command sets all the OSPFv3 AF interfaces as active.

Examples

Setting OSPFv3 AF enabled interfaces as passive:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-ipv4-uc)# passive-interface default
```

Setting OSPFv3 AF enabled interfaces as active:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-ipv4-uc)# no passive-interface default
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute {bgp | connected | host-routes | local loopback | static | ripng |  
    ospf <PROCESS-ID> | ospfv3-af <PROCESS-ID>} [route-map <ROUTE-MAP-NAME>]  
no redistribute {bgp | connected | host-routes | local loopback | static | ripng |  
    ospf <PROCESS-ID> | ospfv3-af <PROCESS-ID>} [route-map <ROUTE-MAP-NAME>]
```

Description

This command redistributes routes originating from other protocols to OSPFv3 AF. This command allows to redistribute routes from other OSPFv3 AF instances. IPv4 address family allows redistribution from other OSPFv3 Ipv4 AFs. IPv6 address family allows redistribution from other OSPFv3 Ipv6 AFs. In addition, if a route-map is specified, then routes that pass the match clause specified in the route-map are only redistributed to OSPFv3 AF. Configuration is not allowed if the referenced route-map has not yet been configured.

Only BGP leaked routes will be given to OSPFv3 AF for redistribution. If you try to redistribute routes from an OSPF process which is not created, user confirmation is asked to create the process before proceeding with redistribution. If accepted, the process is created with defaults and redistribution configuration is applied. If denied, redistribution configuration is skipped.



All the routes added by a routing protocol into RIB are redistributed into the target routing protocol OSPF.

If command **route-redistribute active-routes-only** has been issued, only the routes from other protocols which are selected for forwarding are considered for redistribution into OSPFv3 AF. With the change in redistribute behavior, additional explicit redistribution of connected routes may be needed if any of the deployment assumes redistribution of connected networks will happen via redistribution of dynamic protocol routes into OSPF.

The **no** form of this command disables redistribution of routes to the current OSPFv3 AF process.

Parameter	Description
bgp	Specifies redistributing BGP (Border Gateway Protocol) routes into OSPFv3 AF.
connected	Specifies redistributing connected (directly attached subnet or host).
host-routes	Redistribute dynamic, IVRL and static ARP/ND entries into OSPFv3 AF. ARP/ND entries learnt from EVPN will not be redistributed. The host-routes parameter is applicable to HPE Aruba Networking 8325, 10000, 8360, and 9300/9300S Switch series only.
local loopback	Specifies redistributing local routes of the loopback interface.
static	Specifies redistributing static routes into OSPFv3 AF.
ripng	Specifies redistributing RIPng routes into OSPFv3 AF.
ospf <PROCESS-ID>	Specifies redistributing routes from the specified OSPF process ID. Range: 1 to 65535.

Parameter	Description
ospfv3-af <PROCESS-ID>	Specifies redistributing routes from the specified OSPFv3 AF process ID. Range: 1 to 65535.
route-map <ROUTE-MAP-NAME>	Specifies redistribution filtering by route map. To create a route map, use command route-map .

Examples

Redistributing routes to OSPFv3 AF:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv4-uc) # redistribute bgp
switch(config-ospfv3-ipv4-uc) # redistribute connected
switch(config-ospfv3-ipv4-uc) # redistribute host-routes
switch(config-ospfv3-ipv4-uc) # redistribute static
switch(config-ospfv3-ipv4-uc) # redistribute ripng
switch(config-ospfv3-ipv4-uc) # redistribute ospfv3-af 2
switch(config-ospfv3-ipv4-uc) # redistribute local loopback
switch(config-ospfv3-ipv4-uc) # redistribute static route-map
% Command incomplete.
switch(config-ospfv3-ipv4-uc) # redistribute static route-map static_networks
switch(config-ospfv3-af-1)# redistribute static route-map static_networks1
Route Map static_networks1 not found
switch(config-ospfv3-af-1)# redistribute static route-map static_networks12
Redistribute with route-map config exists
switch(config-ospfv3-ipv4-uc) # redistribute ripng route-map
% Command incomplete.
switch(config-ospfv3-ipv4-uc) # redistribute ripng route-map ripng_networks
switch(config-ospfv3-af-1)# redistribute ripng route-map ripng_networks1
Route Map ripng_networks1 not found
switch(config-ospfv3-af-1)# redistribute ripng route-map ripng_networks12
Redistribute with route-map config exists
switch(config-ospfv3-ipv4-uc) # redistribute ospfv3-af 2 route-map
% Command incomplete.
switch(config-ospfv3-ipv4-uc) # redistribute ospfv3-af 2 route-map tagged_routes
switch(config-ospfv3-ipv4-uc)# redistribute ospfv3-af 2 route-map tagged_routes1
Route Map tagged_routes1 not found
switch(config-ospfv3-ipv4-uc)# redistribute ospfv3-af 2 route-map tagged_routes12
Redistribute with route-map config exists
switch(config-ospfv3-ipv4-uc)# redistribute local loopback route-map
% Command incomplete.
switch(config-ospfv3-ipv4-uc)# redistribute local loopback route-map local_routes
switch(config-ospfv3-af-1)# redistribute local loopback route-map local_routes1
Route Map local_routes1 not found
switch(config-ospfv3-ipv4-uc)# redistribute local loopback route-map local_routes12
Redistribute with route-map config exists
switch(config-ospfv3-ipv4-uc)# redistribute host-routes route-map
% Command incomplete.
switch(config-ospfv3-ipv4-uc)# redistribute host-routes route-map host_routes
switch(config-ospfv3-ipv4-uc)# redistribute host-routes route-map host_routes1
Route Map local_routes1 not found
switch(config-ospfv3-ipv4-uc)# redistribute host-routes route-map host_routes12
Redistribute with route-map config exists
```

Disabling redistributing routes to OSPFv3 AF:

```

switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv6-uc) # no redistribute bgp
switch(config-ospfv3-ipv6-uc) # no redistribute connected
switch(config-ospfv3-ipv6-uc) # no redistribute host-routes
switch(config-ospfv3-ipv6-uc) # no redistribute static
switch(config-ospfv3-ipv6-uc) # no redistribute ripng
switch(config-ospfv3-ipv6-uc) # no redistribute ospfv3-af 2
switch(config-ospfv3-ipv6-uc) # no redistribute local loopback
switch(config-ospfv3-ipv6-uc) # no redistribute static route-map
% Command incomplete.
switch(config-ospfv3-ipv6-uc) # no redistribute static route-map static_networks
switch(config-ospfv3-ipv6-uc) # no redistribute ripng route-map
% Command incomplete.
switch(config-ospfv3-ipv6-uc) # no redistribute ripng route-map ripng_networks
switch(config-ospfv3-ipv6-uc) # no redistribute ospfv3-af 2 route-map
% Command incomplete.
switch(config-ospfv3-ipv6-uc) # no redistribute ospfv3-af 2 route-map tagged_
routes
switch(config-ospfv3-ipv6-uc) # no redistribute local loopback route-map
% Command incomplete.
switch(config-ospfv3-ipv6-uc) # no redistribute local loopback route-map local_
routes
switch(config-ospfv3-ipv6-uc) # no redistribute host-routes route-map
% Command incomplete.
switch(config-ospfv3-ipv6-uc) # no redistribute host-routes route-map host_routes

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

reference-bandwidth

```

reference-bandwidth <BANDWIDTH-VALUE>
no reference-bandwidth

```

Description

Sets the reference bandwidth for OSPFv3 AF. If the OSPFv3 AF interface cost is not explicitly set, then the cost of all the OSPFv3 AF interfaces is recalculated based on the reference bandwidth and link speed of the interface.

For VLAN interfaces the calculated link speed value is 1 Gbps (if the OSPFv3 AF interface cost is not explicitly set).

The **no** form of this command sets the reference bandwidth for OSPFv3 AF to the default of 100000 Mbps.

Parameter	Description
<code><BANDWIDTH-VALUE></code>	Specifies the reference bandwidth used to calculate the cost of an interface in Mbps. Range: 1 to 4000000. Default: 100000.

Examples

Setting the reference bandwidth:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-1)# reference-bandwidth 40000
```

Setting the reference bandwidth to the default value:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-1)# no reference-bandwidth
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3- <code><PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

retransmit-interval

```
retransmit-interval <INTERVAL>
no retransmit-interval
```

Description

Sets the time between retransmitting lost link state advertisements for virtual links.

The **no** form of this command sets the time between retransmitting lost link state advertisements to the default of 5 seconds for virtual links.

Parameter	Description
<code><INTERVAL></code>	Specifies the time interval for the retransmit interval, in seconds. Range: 1 to 3600. Default: 5.

Examples

Setting OSPFv3 AF virtual links retransmit interval:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# retransmit-interval 30
```

Setting OSPFv3 AF virtual links retransmit interval to default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no retransmit-interval
switch(config-router-vlink6)# no retransmit-interval 30
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

router-id

```
router-id <ROUTER-ADDRESS>
no router-id
```

Description

Sets an ID for the router in an IPv4 address format.

Parameter	Description
<ROUTER-ADDRESS>	Specifies the router address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Required
no	Unconfigures the router-id for the instance. The Router-id is changed to the dynamically selected router-id. The default router-id 0.0.0.0 is updated to the routing stack that triggers to auto-elect a router-id based on the highest ip-address of loopback interface or highest ip-address of interfaces. The configuration is supported globally as well as per address-families ipv4-unicast, ipv6-unicast. If address-family specific router-id is configured, it takes precedence over global configuration.



In case there are duplicate loopback IPs within an OSPF domain then the recommendation is to explicitly configure router-id to prevent an unintended IP Address from being selected as router-id. Virtual VTEP is one such example which uses same loopback IP on 2 switches. Even if the IP is not the highest address to be selected as router-id, there switches. Dynamic election of router-id is not supported when multiple OSPF processes are configured on the same VRF. Explicit router-id configuration is required on each OSPF process.

Dynamic router-id is chosen from the list of configured IPs at the time of the router-id election. In Graceful Restart and Management Module failover scenarios, the manual router-id configuration is highly recommended as the router-id should be preserved before and after these events. Graceful Restart would fail if there is a change in the router-id causing traffic loss. A few scenarios where the dynamically elected router-id after a restart could be different from what was selected before daemon restart are mentioned below:



- OSPF selects the router-id. Later on, new interface IPs are configured. OSPF doesn't re-calculate the router-id to consider the newer IP additions. However, after the restart, router-id is again calculated which considers all the IPs (including the ones which were later added).
- After a daemon restart, the router-id is chosen based on the order in which the interface IP notifications are received by the OSPF process. OSPF considers the IP notifications received until it starts the router-id selection. The IP notifications received post the router-id selection are not considered.

Examples

Setting router-id in the OSPFv3 AF context:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1) # router-id 1.1.1.1
switch(config-ospfv3-af-1) # address-family ipv4 unicast
switch(config-ospfv3-ipv4-uc) # router-id 2.2.2.2
switch(config-ospfv3-af-1) # address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc) # router-id 3.3.3.3
```

Unconfiguring router-id:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv4-uc) # no router-id
switch(config-ospfv3-ipv4-uc) # no router-id 1.1.1.1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

router ospfv3-af

```
router ospfv3-af <PROCESS-ID> [vrf <VRF-NAME>]
no router ospfv3-af <PROCESS-ID> [vrf <VRF-NAME>]
```

Description

Creates the OSPFv3 AF process (if not created already) and enters the router OSPFv3 AF instance context. Optionally if specified, you can specify a named VRF, or the default VRF if the <vrf-name> is not specified. Maximum of eight OSPFv3 processes are allowed per VRF.

The switch allows configuration of OSPFv2, OSPFv3, OSPFv3 IPv4 AF and OSPFv3 IPv6 AF. But at any point only 8 OSPF instances can run per address-family, 8 instances for IPv4 (OSPFv2 + OSPFv3 IPv4 AF) and 8 instances for IPv6 (OSPFv3 + OSPFv3 IPv6 AF).

The **no** form of this command removes the OSPFv3 AF instance. If a VRF is specified, it removes the OSPF instance from the named VRF, or the default VRF if the <var-name> is not specified.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID. Length: 1 to 65535.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Entering the router OSPFv3 AF instance:

```
switch(config)# router ospfv3-af 1
```

Setting the router OSPFv3 VRF instance:

```
switch(config)# router ospfv3-af 1 vrf vrf_red
```

Removing the router OSPFv3 AF instance:

```
switch#(config)# no router ospfv3-af 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show ospfv3-af ipv4 statistics

show ospfv3-af [<process-id>] ipv4 statistics [all-vrfs | vrf <vrf-name>]

Description

This command displays the OSPFv3 AF shortest path first (SPF) calculation statistics.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID. Range: 1 to 65535
all-vrfs	Display the OSPFv3 AF statistics information for all the VRFs.
vrf <VRF-NAME>	Specify the VRF name.

Example

```
switch# show ospfv3-af ipv4 statistics
Address-family : IPv4 Unicast
-----
OSPFv3 AF Process ID 1 VRF default, Statistics (cleared 3h 2m 21s ago)
-----
Unknown Interface Drops           : 0
Unknown Virtual Interface Drops   : 0
Bad IPv6 Header Length Drops      : 0
Wrong OSPFv3 Version Drops        : 0
Bad Source IPv6 Drops             : 0
Resource Failure Drops            : 0
Bad Header Length Drops           : 0
Total Drops                      : 0
switch# show ospfv3-af 2 ipv4 statistics vrf red
Address-family : IPv4 Unicast
-----
OSPFv3 AF Process ID 2 VRF red, Statistics (cleared 3h 2m 30s ago)
-----
Unknown Interface Drops           : 0
Unknown Virtual Interface Drops   : 0
Bad IPv6 Header Length Drops      : 0
Wrong OSPFv3 Version Drops        : 0
Bad Source IPv6 Drops             : 0
Resource Failure Drops            : 0
Bad Header Length Drops           : 0
Total Drops                      : 0
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show debug buffer module ospfv3-af

```
show debug buffer module ospfv3-af
[severity (alert|crit|debug|emer|err|info|notice|warn)]
```

Description

Displays debug logs for OSPFv3 AF stored in the specified debug buffer.

Parameter	Description
<MODULE-NAME>	Filters debug logs displayed by the specified module name.
severity (alert crit debug emer err info notice warn)	Displays debug logs for OSPFv3 AF with a specified severity level. Defaults to debug . Optional.
alert	Displays debug logs with a severity level of alert (6) and above.
crit	Displays debug logs with a severity level of critical (5) and above.
debug	Displays debug logs with all severities.
emer	Displays debug logs with a severity level of emergency (7) only.
err	Specifies storage of debug logs with severity level of error (4) and above.
info	Displays debug logs with a severity level of info (1) and above.
notice	Specifies storage of debug logs with severity level of notice (2) and above.
warning	Displays debug logs with a severity level of warning (3) and above.

Examples

```
switch(config)# show debug
```

```
-----
```

module	sub_module	severity	vlan	port	ip	mac	instance
vrf							
ospfv3-af	all	debug					

```

switch(config)# show debug buffer module ospfv3-af
-----
show debug buffer
-----
2017-09-18:10:35:38.621611|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|OSPF
537265152 hitless restart state changed (None -> None),
reason: None.
2017-09-18:10:35:38.621626|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF| (OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.621836|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-
AF|0X01111000 Protocol Manager has initialized successfully.
2017-09-18:10:35:38.621846|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Entity
index
= OSPF 537265152
2017-09-18:10:35:38.621854|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF| (OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.622188|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|OSPF
537265152 hitless restart state changed (None -> None),
reason: None.
2017-09-18:10:35:38.622197|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF| (OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.622423|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|OSPF
537265152 created.
2017-09-18:10:35:38.622433|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF| (OSPFv3
process Id = 0, VRF Name = default)
2017-09-18:10:35:38.622516|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|A master
join has been successfully registered.
2017-09-18:10:35:38.622524|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Join
interface type
= 2
2017-09-18:10:35:38.622536|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Join
interface ID
= 0X00000001
2017-09-18:10:35:38.622544|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF| (OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.622717|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|OSPF
537265152 i/f idx 0X10010101: OSPF has been told over
the I3 interface about a new address on an
2017-09-18:10:35:38.622728|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-
AF|interface, or about updated attributes of an existing address.
2017-09-18:10:35:38.622738|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Address
= 111::1
2017-09-18:10:35:38.622746|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Scope ID
= 268501249
2017-09-18:10:35:38.622754|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Prefix
length
= 64
2017-09-18:10:35:38.622762|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Remote
router address
= ::
2017-09-18:10:35:38.622771|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Address
use flags
= 0X00
2017-09-18:10:35:38.622780|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF| (OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.625212|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|OSPF
537265152 activated successfully
2017-09-18:10:35:38.625225|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|Router
ID
rtr ID 1.1.1.1

```

```

2017-09-18:10:35:38.625235|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|(OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.625286|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|OSPF
537265152 was Down and is now Going Up.
2017-09-18:10:35:38.625295|hpe-routing|LOG_INFO|AMM|-|OSPFV3-AF|OSPFV3-AF|(OSPFv3
process Id = 1, VRF Name = default)
2017-09-18:10:35:38.625309|hpe-routing|LOG_ERR|AMM|-|OSPFV3-AF|OSPFv3_AF_
EVENT|Failed to configure interface cost for stub link port 1/1/1.
2017-09-18:10:35:38.625312|hpe-routing|LOG_ERR|AMM|-|OSPFV3-AF|OSPFv3_AF_
EVENT|Could not send ospfv3VirtNbrStateChange Trap
2020-07-21:11:36:47.324342|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|OSPF 537265152 NM has sent a Hello packet.
2020-07-21:11:36:47.324717|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Sending interface index = i/f idx 0X51101000.
2020-07-21:11:36:47.324952|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Router ID of target neighbor
(null string if sent per interface) = .
2020-07-21:11:36:47.325217|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Destination IP address = IP addr FF02::5.
2020-07-21:11:36:47.325460|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|
(End of packet, OSPFv3 process Id = 1, VRF Name = default)
2020-07-21:11:36:47.326710|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|OSPF message details:
2020-07-21:11:36:47.326946|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Header: Src IP:FE80::800:901:4C3:C58B
Type: 1 Rtr Id:2.2.2.2 Area:0.0.0.1 Inst ID:0
2020-07-21:11:36:47.327166|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Packet: Hello: I/f 0X51101000 Pri:1 Opt:19 Hello
Int:10 Dead Int:40 DR:2.2.2.2 BDR:1.1.1.1
2020-07-21:11:36:47.327350|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|
(End of packet, OSPFv3 process Id = 1, VRF Name = default)
2020-08-12:11:59:50.183653|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|OSPF message details:
2020-08-12:11:59:50.183666|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Header: Src IP:FE80::800:901:4C1:3751 Dst IP:FF02::5
Type: 4 Rtr Id:2.2.2.2 Area:0.0.0.1 Inst ID:0
2020-08-12:11:59:50.183676|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Packet: LS Upd: Num LSAs 2
2020-08-12:11:59:50.183687|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|
(End of packet, OSPFv3 process Id = 1, VRF Name = default)
2020-08-12:11:59:50.272301|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|OSPF message details:
2020-08-12:11:59:50.272313|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Header: Src IP:FE80::800:901:4C1:3751 Dst IP:FF02::5
Type: 5 Rtr Id:2.2.2.2 Area:0.0.0.1 Inst ID:0
2020-08-12:11:59:50.272323|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Packet: LS Ack
2020-08-12:11:59:50.272332|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|
(End of packet, OSPFv3 process Id = 1, VRF Name = default)
2020-08-12:11:59:45.072407|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|OSPF message details:
2020-08-12:11:59:45.072424|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Header: Src IP:FE80::800:901:4C1:3751
Dst IP:FE80::800:901:40D:A274 Type: 2 Rtr Id:2.2.2.2 Area:0.0.0.1 Inst ID:0
2020-08-12:11:59:45.072443|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|Packet: DB Desc: If MTU:1500 Opt:19 I,M,MS
bits:0X01 Seq No:1020993
2020-08-12:11:59:45.072460|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|
(End of packet, OSPFv3 process Id = 1, VRF Name = default)
2020-08-12:11:59:45.073077|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_
PACKET|OSPF message details:

```



```

2020-08-12:11:59:45.073096|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|Header: Src IP:FE80::800:901:4C1:3751
Dst IP:FE80::800:901:40D:A274 Type: 3 Rtr Id:1.1.1.1 Area:0.0.0.1 Inst ID:0
2020-08-12:11:59:45.073114|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|Packet: LS Req: First LS Type:8193 LS id:0.0.0.0
Adv Router:2.2.2.2
2020-08-12:11:59:45.073130|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|(End of packet, OSPFv3 process Id = 1, VRF Name = default)
2020-08-12:12:11:22.344623|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|OSPF message details:
2020-08-12:12:11:22.344635|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|Header: Src IP:FE80::800:901:4C1:3751
Dst IP:FE80::800:901:40D:A274 Type: 2 Rtr Id:2.2.2.2 Area:0.0.0.1 Inst ID:0
2020-08-12:12:11:22.344646|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|Packet: DB Desc: If MTU:1500 Opt:19 I,M,MS bits:0X07
Seq No:1728268
2020-08-12:12:11:22.344663|hpe-routing|LOG_DEBUG|AMM|-|OSPFV3-AF|OSPFv3_AF_PACKET|(End of packet, OSPFv3 process Id = 1, VRF Name = default)

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4

```
show ospfv3-af [<PROCESS-ID>] ipv4 [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows OSPFv3 AF information including area, state, and configuration information.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID optionally to show OSPFv3 AF information for a particular OSPF process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 AF information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. The default VRF OSPFv3 AF process information is displayed if VRF is not mentioned. Default: default.

Example

Showing general OSPFv3 AF configurations:

```
switch# show ospfv3-af 200 ipv4
Address-family : IPv4 Unicast
-----

VRF : default                                Process : 20200
-----

Router ID          : 1.1.1.1                OSPFv3-AF          : Enabled
BFD                : Disabled                SPF Start Interval : 200 ms
SPF Hold Interval  : 1000 ms                 SPF Max Wait Interval : 5000 ms
LSA Start Interval : 5000 ms                 LSA Hold Interval   : 1000 ms
LSA Max Wait Interval : 1000 ms              LSA Arrival Interval : 1000 ms
External LSAs      : 0                      Checksum Sum        : 0
ECMP                : 4                      Reference Bandwidth  : 100000 Mbps
Area Border         : Yes                    AS Border           : No
GR Status           : Enabled                 GR Interval         : 120 sec
GR State            : Inactive                 GR Exit Status      : None
GR Helper           : Enabled                 GR Strict LSA Check  : Enabled
GR Ignore Lost I/F  : Disabled                Internal Process ID  : 1
Summary address:
  prefix fd00::1/64, advertise, tag 10

Area      Total Active
-----
Normal    2          2
Stub      0          0

Area : 0.0.0.0
-----
Area Type          : Normal                Status              : Active
Total Interfaces   : 1                    Active Interfaces   : 1
Passive Interfaces  : 0                    Loopback Interfaces : 0
SPF calculation count : 4
Area ranges:
  fd00::1/64, inter-area, no-advertise
AH Authentication   : SHA1, SPI 256
Number of LSAs      : 5                    Checksum Sum        : 99122

Area : 0.0.0.1
-----
Area Type          : Normal                Status              : Active
Total Interfaces   : 1                    Active Interfaces   : 1
Passive Interfaces  : 0                    Loopback Interfaces : 0

SPF Calculation Count : 4
Area ranges:
  fd00::1/64, inter-area, no-advertise
ESP Authentication  : SHA1
Encryption          : 3DES, SPI 256
Number of LSAs      : 5                    Checksum Sum        : 99122
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4 border-routers

```
show ospfv3-af [<PROCESS-ID>] ipv4 border-routers | [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows the OSPFv3 AF routing table entries for Area Border Router (ABR) and Autonomous System Border Router (ASBR).

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID to show the OSPFv3 AF routing table entries for ABR and ASBR for the particular OSPFv3 AF process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 AF border router information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Showing OSPFv3 AF border routers information for VRF **vrf_red**:

```
switch# show ospfv3-af ipv4 border-routers vrf vrf_red

Address-family : IPv4 Unicast
-----

VRF : vrf_red      Process ID : 1
                Internal Routing Table
-----

Codes: i - Intra-area route, I - Inter-area route
Router-ID Cost  Type   Area   SPF   Nexthop   Interface
i  1.1.1.1    1    ASBR   0.0.0.0  9     10.10.10.1  1/1/2
i  3.3.3.3    1    ASBR   1.1.1.1  9     20.20.20.1  ** tunnel1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4 interface

```
show ospfv3-af [<PROCESS-ID>] ipv4 interface [<INTERFACE-NAME>] | vlan <VLAN-ID> | lag
<LAG-ID> | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>]
[brief] [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 AF enabled IPv4 interfaces.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID optionally to show the OSPFv3 AF enabled interfaces for the particular OSPFv3 AF process. Range: 1 to 65535.
<INTERFACE-NAME>	Selects to show information only for the specified OSPFv3 AF enabled interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
brief	Include this parameter to display a brief overview of the following OSPFv3 AF configuration information. - Interface: OSPFv3 AF interface name. - Area: OSPFv3 AF area ID. - Cost: The metric OSPFv3 AF uses to judge a path's feasibility, calculated as (reference bandwidth / interface bandwidth). - State: Indicates if the interface is a designated router (Dr) or a backup designated router (Backup-dr). - Status: Indicates if the interface is up or down. - Flags: P - Passive A - Active.
all-vrfs	Select to show OSPFv3 AF-enabled interface information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF information for all interfaces in default VRF:

```
switch# show ospfv3-af ipv4 interface
Codes: DR - Designated router BDR - Backup Designated router

Address-family : IPv4 Unicast
-----

Interface 1/1/1 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                                Process          : 1
IP Address         : 1.1.1.2                                Area              :
0.0.0.0
Status            : Up                                      Network Type     :
Broadcast
Hello Interval     : 10      sec                            Dead Interval    : 40
sec
Transit Delay      : 1      sec                            Retransmit Interval : 5
sec
BFD                : Disabled                               Link Speed       :
1000 Mbps
Cost Configured    : 1                                      Cost Calculated  : 4
State/Type         : BDR                                    Router Priority   : 1
DR                 : 3.3.3.3                                BDR              :
1.1.1.3
Link LSAs          : 2                                      Checksum Sum     :
26868
AH Authentication  : SHA1, SPI 256 (Area)                  Passive          : Yes

Interface 1/1/2 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                                Process          : 1
IP Address         : 10.10.10.2                             Area              :
0.0.0.0
Status            : Up                                      Network Type     :
Broadcast
Hello Interval     : 10      sec                            Dead Interval    : 40
sec
Transit Delay      : 1      sec                            Retransmit Interval : 5
sec
Link Speed         : 1000 Mbps
Cost Configured    : 1                                      Cost Calculated  : 4
State/Type         : BDR                                    Router Priority   : 1
DR                 : 10.10.10.2                             BDR              :
10.10.10.1
Link LSAs          : 0                                      Checksum Sum     : 0
AH Authentication  : SHA1, SPI 256 (Area)                  Passive          : No

Interface tunnell is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                                Process          : 1
IPv6 Address       : 10.10.10.1                             Area              :
0.0.0.1
Status            : Up                                      Network Type     :
Broadcast
Hello Interval     : 10      sec                            Dead Interval    : 40
sec
Transit Delay      : 1      sec                            Retransmit Interval : 5
sec
BFD                : Disabled                               Link Speed       :
1000 Mbps
Cost Configured    : 1                                      Cost Calculated  : 4
State/Type         : DR                                    Router Priority   : 1
```

```

DR                : 10.10.10.2                BDR                :
10.10.10.1
Link LSAs         : 1                        Checksum Sum      :
9168
AH Authentication : SHA1, SPI 256 (Area)       Passive           : Yes

Interface vlan10 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process            : 1
IPv6 Address       : 10.10.10.3             Area              :
0.0.0.1
Status            : Up                      Network Type      :
Broadcast
Hello Interval    : 10      sec             Dead Interval     : 40
sec
Transit Delay     : 1      sec             Retransmit Interval : 5
sec
BFD               : Disabled                Link Speed        :
1000 Mbps
Cost Configured   : 1                      Cost Calculated   : 4
State/Type        : DR                     Router Priority    : 1
DR                : 10.10.10.2             BDR               :
10.10.10.1
Link LSAs         : 1                        Checksum Sum      :
9168
AH Authentication : MD5, SPI 257            Passive           : No

Interface vlan20 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process            : 1
IPv6 Address       : 1.1.1.1                Area              :
0.0.0.1
Status            : Up                      Network Type      :
Broadcast
Hello Interval    : 10      sec             Dead Interval     : 40
sec
Transit Delay     : 1      sec             Retransmit Interval : 5
sec
Link Speed        : 1000 Mbps
Cost Configured   : 1                      Cost Calculated   : 4
State/Type        : DR                     Router Priority    : 1
DR                : 1.1.1.3                BDR               : NA
Link LSAs         : 1                        Checksum Sum      :
9168
AH Authentication : MD5, SPI 257            Passive           : No

```

Showing overview information for OSPFv3 AF enabled interfaces for all VRFs in brief:

```

switch# show ospfv3-af ipv4 interface brief all-vrfs
Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 1 VRF default
=====

Total Number of Interfaces: 2

Flags: P - Passive  A - Active

Interface      Area          Cost          State          Status      Flags

```

```

-----
1/1/1          0.0.0.0      1      BDR      Up      P
vlan10         0.0.0.1      1      DR       Up      A

OSPFv3 AF Process ID 2 VRF red
=====

Total Number of Interfaces: 1

Flags: P - Passive  A - Active

Interface      Area          Cost      State      Status      Flags
-----
1/1/2          0.0.0.1      1      BDR      Up      P
tunnell        0.0.0.0      100     DR       Up      A

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4 lsdb

```

show ospfv3-af [<PROCESS-ID>] ipv4 lsdb [all-vrfs | vrf <VRF-NAME>] [router | network |
inter-area-prefix | inter-area-router | as-external | nssa-external | link | intra-area-
prefix]
[area <AREA-ID>] [lsid <LINK-STATE-ID>] [adv-router <ROUTER-ID> | self]
show ospfv3-af [<PROCESS-ID>] ipv4 lsdb [all-vrfs | vrf <VRF-NAME>] database-summary

```

Description

Shows the OSPFv3 AF link state database summary for different OSPFv3 AF LSAs (Link State Advertisement). Use the parameters to get information for a particular LSA.

Parameter	Description
<PROCESS-ID>	Enter an OSPFv3 AF process ID to display general OSPF information for a particular OSPFv3 AF process. Range: 1 to 65535.
all-vrfs vrf <vrf-name>	Select all-vrfs to display general OSPF information for all VRFs, or use the vrf <VRF-NAME> option to display information for a specific VRF.

Parameter	Description
	Optionally select one of the following parameters to filter the link state database information.
as-external	Show external link states (LSA type 5)
database-summary	Select to display the count of each type of LSA and each area in the database. NOTE: The database-summary parameter does not support the area <area-id> , lsid <link-state-id> or adv-router {<router-id> self} parameters.
inter-area-prefix	Show inter-area prefix link states (LSA type 3)
inter-area-router	Show inter-area router link states (LSA type 4)
intra-area-prefix	Show intra-area prefix link states (LSA type 9)
link	Show link states (LSA type 8)
network	Show network LSAs (LSA type 2).
nssa-external	Show NSSA external link states (LSA type 7).
router	Show router LSAs (LSA type 1).
area <AREA-ID>	Select to display information filtered for the specified area in one of the following formats. OSPFv3 AF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPFv3 AF area identifier in decimal format. Value: 0 to 4294967295.
lsid <LINK-STATE-ID>	Select to display information filtered by link state identifier specified in IPv4 address format (A.B.C.D).
adv-router {<ROUTER-ID> self}	Select to display link states for a particular advertising router. Specify either a Router ID of the advertising router or specify self to show self-originated link states.

Examples

Showing OSPFv3 AF link state database (LSDB) general information:

```
switch# show ospfv3-af ipv4 lsdb
Address-family : IPv4 Unicast
-----

OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum  LSID      Link Count  Bits
-----
40.40.40.40     930     0x80000004 0x2ea1    0         3           None
```


50.50.50.50	935	0x80000002	0x8b52	0	1	E
60.60.60.60	943	0x800003c5	0x9854	0	2	None

Network Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Router Count
60.60.60.60	944	0x80000001	0x7179	1360007168	2
50.50.50.50	935	0x80000001	0x516a	19	1

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Prefix
40.40.40.40	929	0x80000001	0x2498	131072	11.0.0.0/8
50.50.50.50	928	0x80000001	0x5b2f	65536	100.100.0.0/16

Inter Area Router Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Destination Router ID
40.40.40.40	929	0x80000001	0x2498	1	33.33.33.33

AS External Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Prefix
40.40.40.40	264	0x80000001	0x24cc4	1	10.10.0.0/16
40.40.40.40	675	0x80000001	0x5b00f	2	11.11.0.0/16

NSSA External Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Prefix
3.3.3.3	264	0x80000001	0x24ac2	1	200.200.0.0/16

Link-local Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Interface
50.50.50.50	264	0x80000001	0x653c4	19	1/1/1

Intra Area Prefix Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Referenced LS Type
Referenced LSID					
50.50.50.50	263	0x80000001	0x1da34	1	0x2001 0
50.50.50.50	264	0x80000001	0x2a45d	1	0x2002 19

Showing AS external link states:

```
switch# show ospfv3-af ipv4 lsdb as-external
Address-family : IPv4 Unicast
-----

OSPF Router with ID (60.60.60.60) (Process ID 1 VRF default)
=====
```

```

AS External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40    264     0x80000001 0x24cc4     1         10.10.0.0/16
40.40.40.40    675     0x80000001 0x5b00f     2         11.11.0.0/16

```

Showing the LSDB database summary:

```

switch# show ospfv3-af ipv4 lsdb database-summary
Address-family : IPv4 Unicast
-----

OSPF Router with ID (10.1.1.1) (Process ID 1 VRF default)
=====

Area 0.0.0.0 database summary
-----
LSA Type      Count
-----
Router        2
Network       1
Inter Area Prefix 1
Inter Area Router 0
NSSA External 0
Link          3
Intra Area Prefix 3
-----
Total         10

Process 1 database summary
-----
LSA Type      Count
-----
Router        2
Network       1
Inter Area Prefix 1
Inter Area Router 0
AS External   2
NSSA External 0
Link          3
Intra Area Prefix 3
-----
Total         12

```

Showing inter-area prefix LSAs:

```

switch# show ospfv3-af ipv4 lsdb inter-area-prefix
Address-family : IPv4 Unicast
-----

OSPF Router with ID (6.6.6.6) (Process ID 1 VRF default)
=====

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40    929     0x80000001 0x2498      131072    1.0.0.0/8

```

```
50.50.50.50      928      0x800000001  0x5b2f      65536      11.11.0.0./16
```

Showing inter-area router LSAs:

```
switch# show ospfv3-af ipv4 lsdB inter-area-router
Address-family : IPv4 Unicast
-----

OSPF Router with ID (60.60.60.60) (Process ID 1 VRF default)
=====

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Destination Router ID
-----
40.40.40.40     929     0x800000001  0x2498     1         33.33.33.33
```

Showing intra-area prefix LSAs:

```
switch# show ospfv3-af ipv4 lsdB intra-area-prefix
Address-family : IPv4 Unicast
-----

OSPF Router with ID (0.0.0.0) (Process ID 1 VRF default)
=====

Intra Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Referenced LS Type
-----
Referenced LSID
-----
50.50.50.50     263     0x800000001  0x1da34     1         0x2001
0
50.50.50.50     264     0x800000001  0x2a45d     1         0x2002
19
```

Showing link LSAs:

```
switch# show ospfv3-af ipv4 lsdB link
Address-family : IPv4 Unicast
-----

OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

Link-local Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Interface
-----
50.50.50.50     264     0x800000001  0x653c4     19        1/1/1

Link-local Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Interface
-----
```

50.50.50.50	264	0x80000001	0xad324	20	1/1/2

Showing network LSAs:

```
switch# show ospfv3-af ipv4 lsd network
Address-family : IPv4 Unicast
-----

OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Network Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID        Router Count
-----
60.60.60.60    944     0x80000001 0x7179     1360007168  2
50.50.50.50    935     0x80000001 0x516a     19          1
```

Showing NSSA external link states:

```
switch# show ospfv3-af ipv4 lsd nssa-external
Address-family : IPv4 Unicast
-----

OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

NSSA External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID        Prefix
-----
3.3.3.3         264     0x80000001 0x24ac2     1           200.200.0.0/16
```

Showing router LSAs:

```
switch# show ospfv3-af ipv4 lsd router
Address-family : IPv4 Unicast
-----

OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID        Link Count  Bits
-----
40.40.40.40     930     0x80000004 0x2ea1     0           3           None
50.50.50.50     935     0x80000002 0x8b52     0           1           E
60.60.60.60     943     0x800003c5 0x9854     0           2           None
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4 neighbors

```
show ospfv3-af [<PROCESS-ID>] ipv4 neighbors [<NEIGHBOR-ID>]
  [interface <INTERFACE-NAME> | vlan <VLAN-ID> | lag <LAG-ID> | loopback <LOOPBACK-ID> |
  tunnel <TUNNEL-ID>]
  [detail | summary] [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 AF neighbors.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID to show OSPFv3 AF neighbor information for the particular OSPFv3 AF process. Range: 1 to 65535.
neighbors <NEIGHBOR-ID>	Shows information about a particular neighbor, specified in IPv4 format (A.B.C.D).
interface <INTERFACE-NAME>	Shows neighbor information only for the specified interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
detail	Shows detailed information for the neighbors.
summary	Shows summary information for the neighbors.
all-vrfs	Shows neighbor information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF neighbor information for the specified interface:

```

switch# show ospfv3-af ipv4 neighbors 3.3.3.3
Address-family : IPv4 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                    Area          : 0.0.0.0
Interface      : 1/1/1                      Address        : 1.1.1.1
State          : FULL                       Neighbor Priority : 1
Dead Timer Due  : 00:00:36                  Options       : 0x13
Time since last state change : 00h:14m:45s

```

Showing detail OSPFv3 AF neighbor information:

```

switch# show ospfv3-af ipv4 neighbors 3.3.3.3 detail
Address-family : IPv4 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                    Area          : 0.0.0.0
Interface      : 1/1/1                      Address        : 1.1.1.1
State          : FULL                       Neighbor Priority : 1
DR             : 3.3.3.3                    BDR           : 1.1.1.3
Dead Timer Due  : 00:00:36                  Options       : 0x13
Retransmission Queue Length : 0
Time Since Last State Change : 00h:14m:45s

```

Showing OSPFv3 AF neighbor information for interface 1/1/1:

```

switch# show ospfv3-af ipv4 neighbors 3.3.3.3 interface 1/1/1
Address-family : IPv4 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                    Area          : 0.0.0.0
Interface      : 1/1/1                      Address        : 1.1.1.1
State          : FULL                       Neighbor Priority : 1
Dead Timer Due  : 00:00:36                  Options       : 0x13
Time Since Last State Change : 00h:14m:45s

```

Showing OSPFv3 AF neighbor information for tunnel interface:

```

switch# show ospfv3-af ipv4 neighbors 3.3.3.3
Address-family : IPv4 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                    Area          : 0.0.0.0
Interface      : tunnell                    Address        : 1.1.1.1
State          : FULL                       Neighbor Priority : 1
Dead Timer Due  : 00:00:36                  Options       : 0x13
Time since last state change : 00h:14m:45s

```

Showing detail OSPFv3 AF neighbor information for tunnel interface:

```

switch# show ospfv3-af ipv4 neighbors 3.3.3.3 detail
Address-family : IPv4 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                    Area          : 0.0.0.0
Interface      : tunnell                    Address       : 1.1.1.1
State          : FULL                      Neighbor Priority : 1
DR             : 3.3.3.3                    BDR           : 1.1.1.3
Dead Timer Due  : 00:00:36                  Options      : 0x13
Retransmission Queue Length : 0
Time Since Last State Change : 00h:14m:45s

```

Showing summary OSPFv3 AF neighbors information for a specific neighbor for all VRFs:

```

switch# show ospfv3-af ipv4 neighbors 3.3.3.3 summary all-vrfs
Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Neighbor Summary
=====

Interface      Down Attempt Init TwoWay ExStart Exchange Loading Full Total
-----
1/1/1          0    0      0    0      0      0      0      1    1
Total          0    0      0    0      0      0      0      1    1

OSPFv3 AF Process ID 1 VRF red, Neighbor Summary
=====

Interface      Down Attempt Init TwoWay ExStart Exchange Loading Full Total
-----
1/1/2          0    0      0    0      0      0      0      1    1
Total          0    0      0    0      0      0      0      1    1

```

Showing OSPFv3 AF neighbors information for VRF red:

```

switch# show ospfv3-af ipv4 neighbors vrf red
Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 2 VRF red
=====

Total Number of Neighbors: 1

Neighbor ID      Priority  State          Interface
-----
4.4.4.4          1      FULL/DR        1/1/2
Neighbor address 1.1.1.1

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4 routes

```
show ospfv3-af [<PROCESS-ID>] ipv4 routes [<PREFIX/LENGTH>]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows the OSPFv3 AF routing table information.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID that shows information from the OSPFv3 AF routing table for the particular OSPFv3 AF process. Range: 1 to 65535.
<PREFIX/LENGTH>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
all-vrfs	Select to show OSPFv3 AF routing table information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF routing table information:

```
switch# show ospfv3-af ipv4 routes
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Routing Table
-----

Total Number of OSPFv3 AF Routes : 3

11.11.0.0/16      (i) area:0.0.0.0
    directly attached to interface 1/1/1, cost 1 distance 110
200.200.0.0/16    (i) area:0.0.0.0
    directly attached to interface tunnell1, cost 100 distance 110
1.1.1.1/132       (i) area:0.0.0.1
    directly attached to interface vlan10, cost 1 distance 110
```


Showing OSPFv3 AF routing table information for VRF red:

```
switch# show ospfv3-af ipv4 routes vrf red

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 2 VRF red, Routing Table
-----

Total Number of OSPFv3 AF Routes : 1

2.2.2.1/24          (i) area:0.0.0.1
    directly attached to interface 1/1/2, cost 1 distance 110
```

Showing OSPFv3 AF routing table information for destination prefix 2.2.2.1/24:

```
switch# show ospfv3-af 1 ipv4 routes 2.2.2.1/24

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Routing Table for prefixes 2.2.2.1/24
-----

Total Number of OSPFv3 AF Routes : 1

2.2.2.1/24          (i) area:0.0.0.1
    directly attached to interface vlan10, cost 1 distance 110
```

Showing OSPFv3 AF routing table information for destination prefix 200.0.0.0/8:

```
switch# show ospfv3-af 1 ipv4 routes 200.0.0.0/8

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Routing Table for prefixes 200.0.0.0/8
-----

Total Number of OSPFv3 AF Routes : 1

200.0.0.0/8         (i) area:0.0.0.0
    directly attached to interface tunnell1, cost 100 distance 110
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv4 statistics interface

```
show ospfv3-af [<PROCESS-ID>] ipv4 statistics interface [<INTERFACE-NAME>] | vlan <VLAN-ID> | lag <LAG-ID> | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>]
[brief] [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 AF enabled IPv4 interfaces.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID optionally to show the OSPFv3 AF enabled interfaces for the particular OSPFv3 AF process. Range: 1 to 65535.
<INTERFACE-NAME>	Selects to show information only for the specified OSPFv3 AF enabled interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
brief	Include this parameter to display a brief overview of the following OSPFv3 AF configuration information. - Interface: OSPFv3 AF interface name. - Area: OSPFv3 AF area ID. - Cost: The metric OSPFv3 AF uses to judge a path's feasibility, calculated as (reference bandwidth / interface bandwidth). - State: Indicates if the interface is a designated router (Dr) or a backup designated router (Backup-dr). - Status: Indicates if the interface is up or down. - Flags: P - Passive A - Active.
all-vrfs	Select to show OSPFv3 AF-enabled interface information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF information for all interfaces in default VRF:

```
switch# show ospfv3-af ipv4 interface
Codes: DR - Designated router BDR - Backup Designated router

Address-family : IPv4 Unicast
-----

Interface 1/1/1 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process                : 1
IP Address          : 1.1.1.2                Area                  :
0.0.0.0
Status              : Up                    Network Type          :
Broadcast
Hello Interval      : 10      sec             Dead Interval          : 40
sec
Transit Delay       : 1      sec             Retransmit Interval   : 5
sec
BFD                 : Disabled              Link Speed             :
1000 Mbps
Cost Configured     : 1                    Cost Calculated        : 4
State/Type          : BDR                    Router Priority        : 1
DR                  : 3.3.3.3                BDR                   :
1.1.1.3
Link LSAs           : 2                    Checksum Sum           :
26868
AH Authentication   : SHA1, SPI 256 (Area)      Passive               : Yes

Interface 1/1/2 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process                : 1
IP Address          : 10.10.10.2             Area                  :
0.0.0.0
Status              : Up                    Network Type          :
Broadcast
Hello Interval      : 10      sec             Dead Interval          : 40
sec
Transit Delay       : 1      sec             Retransmit Interval   : 5
sec
Link Speed          : 1000 Mbps
Cost Configured     : 1                    Cost Calculated        : 4
State/Type          : BDR                    Router Priority        : 1
DR                  : 10.10.10.2            BDR                   :
10.10.10.1
Link LSAs           : 0                    Checksum Sum           : 0
AH Authentication   : SHA1, SPI 256 (Area)      Passive               : No

Interface tunnell is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process                : 1
IPv6 Address        : 10.10.10.1             Area                  :
0.0.0.1
Status              : Up                    Network Type          :
Broadcast
Hello Interval      : 10      sec             Dead Interval          : 40
sec
Transit Delay       : 1      sec             Retransmit Interval   : 5
sec
BFD                 : Disabled              Link Speed             :
1000 Mbps
Cost Configured     : 1                    Cost Calculated        : 4
State/Type          : DR                    Router Priority        : 1
```

```

DR                : 10.10.10.2                BDR                :
10.10.10.1
Link LSAs         : 1                        Checksum Sum       :
9168
AH Authentication : SHA1, SPI 256 (Area)       Passive            : Yes

Interface vlan10 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process              : 1
IPv6 Address       : 10.10.10.3             Area                 :
0.0.0.1
Status            : Up                      Network Type         :
Broadcast
Hello Interval     : 10      sec             Dead Interval        : 40
sec
Transit Delay      : 1      sec             Retransmit Interval  : 5
sec
BFD                : Disabled                Link Speed           :
1000 Mbps
Cost Configured    : 1                      Cost Calculated      : 4
State/Type         : DR                      Router Priority       : 1
DR                 : 10.10.10.2              BDR                  :
10.10.10.1
Link LSAs         : 1                        Checksum Sum         :
9168
AH Authentication : MD5, SPI 257             Passive              : No

Interface vlan20 is up, Line Protocol is up, Instance Id 64
-----
VRF                : default                Process              : 1
IPv6 Address       : 1.1.1.1                Area                 :
0.0.0.1
Status            : Up                      Network Type         :
Broadcast
Hello Interval     : 10      sec             Dead Interval        : 40
sec
Transit Delay      : 1      sec             Retransmit Interval  : 5
sec
Link Speed         : 1000 Mbps
Cost Configured    : 1                      Cost Calculated      : 4
State/Type         : DR                      Router Priority       : 1
DR                 : 1.1.1.3                BDR                  : NA
Link LSAs         : 1                        Checksum Sum         :
9168
AH Authentication : MD5, SPI 257             Passive              : No

```

Showing overview information for OSPFv3 AF enabled interfaces for all VRFs in brief:

```

switch# show ospfv3-af ipv4 interface
Address-family : IPv4 Unicast
-----

OSPFv3 AF Process ID 1 VRF default
=====

Total Number of Interfaces: 2

Flags: P - Passive  A - Active

Interface      Area          Cost          State          Status      Flags

```

```

-----
1/1/1          0.0.0.0      1      BDR      Up      P
vlan10         0.0.0.1      1      DR       Up      A

OSPFv3 AF Process ID 2 VRF red
=====

Total Number of Interfaces: 1

Flags: P - Passive  A - Active

Interface      Area          Cost      State      Status      Flags
-----
1/1/2          0.0.0.1      1         BDR        Up          P
tunnell        0.0.0.0      100       DR         Up          A

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6

`show ospfv3-af [<PROCESS-ID>] ipv6 [all-vrfs | vrf <VRF-NAME>]`

Description

Shows OSPFv3 AF information including area, state, and configuration information.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID optionally to show OSPFv3 AF information for a particular OSPF process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 AF information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. The default VRF OSPFv3 AF process information is displayed if VRF is not mentioned. Default: default.

Example

Showing general OSPFv3 AF configurations:

```

switch# show ospfv3-af 200 ipv6
Address-family : IPv6 Unicast
-----

VRF : default                                Process : 20200
-----

Router ID          : 1.1.1.1                OSPFv3-AF          : Enabled
BFD                : Disabled                SPF Start Interval : 200 ms
SPF Hold Interval  : 1000 ms                 SPF Max Wait Interval : 5000 ms
LSA Start Interval : 5000 ms                 LSA Hold Interval   : 1000 ms
LSA Max Wait Interval : 1000 ms              LSA Arrival Interval : 1000 ms
External LSAs      : 0                      Checksum Sum        : 0
ECMP                : 4                      Reference Bandwidth  : 100000 Mbps
Area Border         : Yes                    AS Border           : No
GR Status           : Enabled                GR Interval         : 120 sec
GR State            : Inactive               GR Exit Status      : None
GR Helper           : Enabled                GR Strict LSA Check  : Enabled
GR Ignore Lost I/F  : Disabled               Internal Process ID  : 1
Summary address:
    prefix fd00::1/64, advertise, tag 10

Area      Total Active
-----
Normal    2          2
Stub      0          0

Area : 0.0.0.0
-----
Area Type          : Normal                Status              : Active
Total Interfaces   : 1                    Active Interfaces   : 1
Passive Interfaces : 0                    Loopback Interfaces : 0
SPF calculation count : 4
Area ranges:
    fd00::1/64, inter-area, no-advertise
AH Authentication   : SHA1, SPI 256
Number of LSAs      : 5                    Checksum Sum        : 99122

Area : 0.0.0.1
-----
Area Type          : Normal                Status              : Active
Total Interfaces   : 1                    Active Interfaces   : 1
Passive Interfaces : 0                    Loopback Interfaces : 0

SPF Calculation Count : 4
Area ranges:
    fd00::1/64, inter-area, no-advertise
ESP Authentication  : SHA1
Encryption          : 3DES, SPI 256
Number of LSAs      : 5                    Checksum Sum        : 99122

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 border-routers

show ospfv3-af [<PROCESS-ID>] ipv6 border-routers | [all-vrfs | vrf <VRF-NAME>]

Description

Shows the OSPFv3 AF routing table entries for Area Border Router (ABR) and Autonomous System Border Router (ASBR).

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID to show the OSPFv3 AF routing table entries for ABR and ASBR for the particular OSPFv3 AF process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 AF border router information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Showing OSPFv3 AF border routers information for VRF **vrf_red**:

```
switch# show ospfv3-af ipv6 border-routers vrf vrf_red

Address-family : IPv6 Unicast
-----

VRF : vrf_red      Process ID : 1
      Internal Routing Table
-----

Codes: i - Intra-area route, I - Inter-area route
Router-ID Cost  Type   Area   SPF  Nexthop                      Interface
i  1.1.1.1    1    ASBR   0.0.0.0 9    fe80::7272:cfff:fe9a:a15d    1/1/2
i  3.3.3.3    1    ASBR   1.1.1.1 9    fe80::7272:cfff:fe1f:d80    ** tunnel1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 interface

```
show ospfv3-af [<PROCESS-ID>] ipv6 interface [<INTERFACE-NAME>] | vlan <vlan id> |
lag <lag id> | loopback <loopback id> | tunnel <tunnel id>] [brief]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 AF enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID optionally to show the OSPFv3 AF enabled interfaces for the particular OSPFv3 AF process. Range: 1 to 65535.
<INTERFACE-NAME>	Selects to show information only for the specified OSPFv3 AF enabled interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG-ID>	Specifies the lag interface name.
loopback <LOOPBACK-ID>	Specifies the loopback interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
brief	Include this parameter to display a brief overview of the following OSPFv3 AF configuration information. - Interface: OSPFv3 AF interface name. - Area: OSPFv3 AF area ID. - Cost: The metric OSPFv3 AF uses to judge a path's feasibility, calculated as (reference bandwidth / interface bandwidth). - State: Indicates if the interface is a designated router (Dr) or a backup designated router (Backup-dr). - Status: Indicates if the interface is up or down. - Flags: P - Passive A - Active.
all-vrfs	Select to show OSPFv3 AF-enabled interface information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF information for all interfaces in default VRF:

```
switch# show ospfv3-af ipv6 interface
Codes: DR - Designated router  BDR - Backup Designated router
```


Interface 1/1/1 is Up, Line Protocol is Up, Instance ID 10

```
-----
VRF                : default                      Process                : 1
IPv6 address       : fe80::7272:cfff:fe70:67ae      Area                  :
0.0.0.0
Status            : Up                            Network Type          :
Broadcast
Hello Interval    : 10      sec                    Dead Interval         : 40
sec
Transit Delay     : 1      sec                    Retransmit Interval   : 5
sec
BFD               : Disabled                      Link Speed            : 1000
Mbps
Cost Configured   : 1                            Cost Calculated       : 4
State/Type        : BDR                          Router Priority       : 1
DR               : 3.3.3.3                        BDR                  :
1.1.1.3
Link LSAs         : 2                            Checksum Sum          :
26868
AH Authentication : SHA1, SPI 256 (Area)           Passive               : Yes
```

Codes: DR - Designated router BDR - Backup Designated router

Interface 1/1/2 is Up, Line Protocol is Up, Instance ID 70

```
-----
VRF                : default                      Process                : 1
IPv6 address       : fe80::7272:cfff:fe70:67ae      Area                  :
0.0.0.0
Status            : Up                            Network Type          :
Broadcast
Hello Interval    : 10      sec                    Dead Interval         : 40
sec
Transit Delay     : 1      sec                    Retransmit Interval   : 5
sec
BFD               : Disabled                      Link Speed            : 1000
Mbps
Cost Configured   : 1                            Cost Calculated       : 4
State/Type        : BDR                          Router Priority       : 1
DR               : 10.10.10.2                     BDR                  :
10.10.10.1
Link LSAs         : 0                            Checksum Sum          : 0
AH Authentication : SHA1, SPI 256 (Area)           Passive               : No
```

Codes: DR - Designated router BDR - Backup Designated router

Interface tunnell is Up, Line Protocol is Up, Instance ID 70

```
-----
VRF                : default                      Process                : 1
IPv6 address       : fe80::7272:cfff:fe70:679ae      Area                  :
0.0.0.1
Status            : Up                            Network Type          :
Broadcast
Hello Interval    : 10      sec                    Dead Interval         : 40
sec
Transit Delay     : 1      sec                    Retransmit Interval   : 5
sec
BFD               : Disabled                      Link Speed            : 1000
Mbps
Cost Configured   : 1                            Cost Calculated       : 4
State/Type        : DR                          Router Priority       : 1
DR               : 10.10.10.2                     BDR                  :
```

```

10.10.10.1
Link LSAs          : 1                      Checksum Sum      : 9168
AH Authentication  : SHA1, SPI 256 (Area)    Passive            : Yes

Codes: DR - Designated router  BDR - Backup Designated router

Interface vlan10 is Up, Line Protocol is Up, Instance ID 10
-----
VRF                : default                Process            : 1
IPv6 address       : fe80::7272:cfff:fe70:67ae Area            :
0.0.0.1
Status            : Up                     Network Type      :
Broadcast
Hello Interval     : 10      sec            Dead Interval     : 40
sec
Transit Delay      : 1      sec            Retransmit Interval : 5
sec
BFD                : Disabled              Link Speed        : 1000
Mbps
Cost Configured    : 1                    Cost Calculated   : 4
State/Type         : DR                    Router Priority    : 1
DR                 : 10.10.10.2            BDR               :
10.10.10.1
Link LSAs          : 1                      Checksum Sum      : 9168
AH Authentication  : MD5, SPI 257          Passive            : No

Codes: DR - Designated router  BDR - Backup Designated router

Interface vlan20 is Up, Line Protocol is Up, Instance ID 10
-----
VRF                : default                Process            : 1
IPv6 address       : fe80::7272:cfff:fe70:67ae Area            :
0.0.0.1
Status            : Up                     Network Type      :
Broadcast
Hello Interval     : 10      sec            Dead Interval     : 40
sec
Transit Delay      : 1      sec            Retransmit Interval : 5
sec
BFD                : Disabled              Link Speed        : 1000
Mbps
Cost Configured    : 1                    Cost Calculated   : 4
State/Type         : DR                    Router Priority    : 1
DR                 : 1.1.1.3              BDR               : NA
Link LSAs          : 1                      Checksum Sum      : 9168
AH Authentication  : MD5, SPI 257          Passive            : No

```

Showing overview information for OSPFv3 AF enabled interfaces for all VRFs in brief:

```

switch# show ospfv3-af ipv6 interface brief all-vrfs
VRF : default                Process : 1
=====

Total Number of Interfaces: 2

Flags: P - Passive  A - Active

Interface      Area          Cost      State      Status      Flags
-----
1/1/1         0.0.0.0       1         BDR        Up          P

```

```
vlan10          0.0.0.1          1          DR          Up          A
```

```
VRF : red          Process : 1
```

```
=====
```

```
Total Number of Interfaces: 1
```

```
Flags: P - Passive  A - Active
```

Interface	Area	Cost	State	Status	Flags
1/1/2	0.0.0.1	1	BDR	Up	P
tunnell	0.0.0.0	100	DR	Up	A



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 lsdb

```
show ospfv3-af [<process-id>] ipv6 lsdb
adv-router {<ROUTER-ID>|self}
area <AREA-ID>
lsid <link-state-id>
all-vrfs|vrf <VRF-NAME>}
as-external
asbr-summary
database-summary
inter-area-prefix
inter-area-router
intra-area-prefix
link
network
nssa-external
router
summary
```

Description

Shows the OSPFv3 AF link state database summary for different OSPF LSAs (Link State Advertisement). Use the parameters to get information for a particular LSA.

Parameter	Description
<code><PROCESS-ID></code>	Enter an OSPFv3 AF process ID to display general OSPF information for a particular OSPF process. Range: 1 to 65535.
<code>adv-router {<ROUTER-ID> self}</code>	Select to display link states for a particular advertising router. Specify either a Router ID of the advertising router or specify self to show self-originated link states.
<code>area <AREA-ID></code>	Select to display information filtered for the specified area in one of the following formats. OSPFv3 AF area identifier in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. OSPFv3 AF area identifier in decimal format. Value: 0 to 4294967295.
<code>lsid <LINK-STATE-ID></code>	Select to display information filtered by link state identifier specified in IPv4 address format (A.B.C.D).
<code>all-vrfs {vrf <vrf-name>}</code>	Select all-vrfs to display general OSPF information for all VRFs, or use the vrf <VRF-NAME> option to display information for a specific VRF. Optionally select one of the following parameters to filter the link state database information.
<code>as-external</code>	Show external link states (LSA type 5)
<code>database-summary</code>	Select to display the count of each type of LSA and each area in the database. NOTE: The database-summary parameter does not support the area <area-id> , lsid <link-state-id> or adv-router {<router-id> self} parameters.
<code>inter-area-prefix</code>	Show inter-area prefix link states (LSA type 3)
<code>inter-area-router</code>	Show inter-area router link states (LSA type 4)
<code>intra-area-prefix</code>	Show intra-area prefix link states (LSA type 9)
<code>link</code>	Show link states (LSA type 8)
<code>network</code>	Show network LSAs (LSA type 2).
<code>nssa-external</code>	Show NSSA external link states (LSA type 7).
<code>router</code>	Show router LSAs (LSA type 1).

Examples

Showing OSPFv3 AF link state database (LSDB) general information:

```
switch# show ospfv3-af ipv6 lsdb
Address-family : IPv6 Unicast
-----
```

OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)

=====

Router Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Link Count	Bits
40.40.40.40	930	0x80000004	0x2ea1	0	3	None
50.50.50.50	935	0x80000002	0x8b52	0	1	E
60.60.60.60	943	0x800003c5	0x9854	0	2	None

Network Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Router Count
60.60.60.60	944	0x80000001	0x7179	1360007168	2
50.50.50.50	935	0x80000001	0x516a	19	1

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Prefix
40.40.40.40	929	0x80000001	0x2498	131072	FEC0:3344::/32
50.50.50.50	928	0x80000001	0x5b2f	65536	111::/64

Inter Area Router Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Destination Router ID
40.40.40.40	929	0x80000001	0x2498	1	33.33.33.33

AS External Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Prefix
40.40.40.40	264	0x80000001	0x24cc4	1	10::/64
40.40.40.40	675	0x80000001	0x5b00f	2	11::/64

NSSA External Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Prefix
3.3.3.3	264	0x80000001	0x24ac2	1	200::/64

Link-local Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Interface
50.50.50.50	264	0x80000001	0x653c4	19	1/1/1

Intra Area Prefix Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Referenced LS Type
Referenced LSID					
50.50.50.50	263	0x80000001	0x1da34	1	0x2001 0
50.50.50.50	264	0x80000001	0x2a45d	1	0x2002 19

Showing AS external link states:

```
switch# show ospfv3-af ipv6 lsd as-external

Address-family : IPv6 Unicast
-----

OSPF Router with ID (60.60.60.60) (Process ID 1 VRF default)
=====

AS External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID      Prefix
-----
40.40.40.40     264     0x80000001 0x24cc4     1         10::/64
40.40.40.40     675     0x80000001 0x5b00f     2         11::/64
```

Showing the LSDB database summary:

```
switch# show ospfv3-af ipv6 lsd database-summary

Address-family : IPv6 Unicast
-----

OSPF Router with ID (10.1.1.1) (Process ID 1 VRF default)
=====

Area 0.0.0.0 database summary
-----
LSA Type      Count
-----
Router        2
Network       1
Inter Area Prefix 1
Inter Area Router 0
NSSA External 0
Link          3
Intra Area Prefix 3
-----
Total         10

Process 1 database summary
-----
LSA Type      Count
-----
Router        2
Network       1
Inter Area Prefix 1
Inter Area Router 0
AS External   2
NSSA External 0
Link          3
Intra Area Prefix 3
-----
Total         12
```

Showing inter-area prefix LSAs:

```
switch# show ospfv3-af ipv6 lsd inter-area-prefix

Address-family : IPv6 Unicast
```

```

-----
OSPF Router with ID (6.6.6.6) (Process ID 1 VRF default)
=====

Inter Area Prefix Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID        Prefix
-----
40.40.40.40     929     0x80000001 0x2498      131072      FEC0:3344::/32
50.50.50.50     928     0x80000001 0x5b2f      65536       111::/64

```

Showing network LSAs:

```

switch# show ospfv3-af ipv6 lsdbs network

Address-family : IPv6 Unicast
-----

OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Network Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID        Router Count
-----
60.60.60.60     944     0x80000001 0x7179      1360007168  2
50.50.50.50     935     0x80000001 0x516a      19          1

```

Showing NSSA external link states:

```

switch# show ospfv3-af ipv6 lsdbs nssa-external

Address-family : IPv6 Unicast
-----

OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

NSSA External Link State Advertisements (Area 0.0.0.0)
-----
ADV Router      Age      Seq#      Checksum    LSID        Prefix
-----
3.3.3.3         264     0x80000001 0x24ac2     1           200::/64

```

Showing router LSAs:

```

switch# show ospfv3-af ipv6 lsdbs router

Address-family : IPv6 Unicast
-----

OSPF Router with ID (50.50.50.50) (Process ID 1 VRF default)
=====

Router Link State Advertisements (Area 0.0.0.0)
-----

```

ADV Router	Age	Seq#	Checksum	LSID	Link Count	Bits
40.40.40.40	930	0x80000004	0x2ea1	0	3	None
50.50.50.50	935	0x80000002	0x8b52	0	1	E
60.60.60.60	943	0x800003c5	0x9854	0	2	None

Showing inter-area router LSAs:

```
switch# show ospfv3-af ipv6 lsdB inter-area-router
```

Address-family : IPv6 Unicast

OSPF Router with ID (60.60.60.60) (Process ID 1 VRF default)
=====

Inter Area Router Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Destination Router ID
40.40.40.40	929	0x80000001	0x2498	1	33.33.33.33

Showing link states:

```
switch# show ospfv3-af ipv6 lsdB link
```

Address-family : IPv6 Unicast

OSPF Router with ID (2.2.2.1) (Process ID 1 VRF default)
=====

Link-local Link State Advertisements (Area 0.0.0.0)

ADV Router	Age	Seq#	Checksum	LSID	Interface
50.50.50.50	264	0x80000001	0x653c4	19	1/1/1

Link-local Link State Advertisements (Area 0.0.0.1)

ADV Router	Age	Seq#	Checksum	LSID	Interface
50.50.50.50	264	0x80000001	0xad324	20	1/1/2

Showing lintra-area prefix LSAs:

```
switch# show ospfv3-af ipv6 lsdB intra-area-prefix
```

Address-family : IPv6 Unicast

OSPF Router with ID (0.0.0.0) (Process ID 1 VRF default)
=====

Intra Area Prefix Link State Advertisements (Area 0.0.0.0)

ADV Router Referenced LSID	Age	Seq#	Checksum	LSID	Referenced LS	Type

50.50.50.50	263	0x80000001	0x1da34	1	0x2001	0
50.50.50.50	264	0x80000001	0x2a45d	1	0x2002	19



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 neighbors

```
show ospfv3-af [<PROCESS-ID>] ipv6 neighbors [<NEIGHBOR-ID>]
  [interface <INTERFACE-NAME>] | vlan <VLAN ID> | lag <LAG ID> | loopback <LOOPBACK ID>
  | tunnel<tunnel id>][detail | summary]
  [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows information about OSPFv3 AF neighbors.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID to show OSPFv3 AF neighbor information for the particular OSPFv3 AF process. Range: 1 to 65535.
neighbors <NEIGHBOR-ID>	Shows information about a particular neighbor, specified in IPv4 format (A.B.C.D).
interface <INTERFACE-NAME>	Shows neighbor information only for the specified interface.
detail	Shows detailed information for the neighbors.
summary	Shows summary information for the neighbors.
lag <LAG ID>	Specifies lag interface name.
loopback <LOOPBACK ID>	Specifies the vlan interface name.

Parameter	Description
all-vrfs	Shows neighbor information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF neighbors information:

```
switch# show ospfv3-af ipv6 neighbors
Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default
=====

Total Number of Neighbors: 1

Neighbor ID      Priority   State             Interface
-----
3.3.3.3          1         FULL/DR           1/1/1
Neighbor address fe80::7272:cfff:fe79:7510
```

Showing OSPFv3 AF neighbors information for neighbor 3.3.3.3:

```
switch# show ospfv3-af ipv6 neighbors 3.3.3.3
Address-family : IPv6 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                      Area          : 0.0.0.0
Interface      : 1/1/1                        Address       :
fe80::7272:cfff:fe79:7510
State          : FULL                          Neighbor Priority : 1
Dead Timer Due : 00:00:36                      Options       : 0x13
Time since last state change : 00h:14m:45s
```

Showing detail OSPFv3 AF neighbors information for neighbor 3.3.3.3:

```
switch# show ospfv3-af ipv6 neighbors 3.3.3.3 detail
Address-family : IPv6 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                      Area          : 0.0.0.0
Interface      : 1/1/1                        Address       :
fe80::7272:cfff:fe79:7510
State          : FULL                          Neighbor Priority : 1
DR             : 3.3.3.3                      BDR           : 1.1.1.3
Dead Timer Due : 00:00:36                      Options       : 0x13
Retransmission Queue Length : 0
Time Since Last State Change : 00h:14m:45s
```

Showing OSPFv3 AF neighbors information for interface 1/1/1:

```
switch# show ospfv3-af ipv6 neighbors 3.3.3.3 interface 1/1/1

Address-family : IPv6 Unicast
-----

VRF : default                                Process : 1
-----
Router-Id      : 3.3.3.3                    Area       : 0.0.0.0
Interface     : 1/1/1                      Address      :
fe80::7272:cfff:fe79:7510
State         : FULL                        Neighbor Priority : 1
Dead Timer Due : 00:00:36                  Options      : 0x13
Time Since Last State Change : 00h:14m:45s
```

Showing summary OSPFv3 AF neighbors information for a specific neighbor for all VRFs:

```
switch# show ospfv3-af ipv6 neighbors 3.3.3.3 summary all-vrfs

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Neighbor Summary
=====

Interface      Down Attempt Init TwoWay ExStart Exchange Loading Full Total
-----
1/1/1          0    0      0    0      0      0      0      1    1
Total          0    0      0    0      0      0      0      1    1

OSPFv3 AF Process ID 1 VRF red, Neighbor Summary
=====

Interface      Down Attempt Init TwoWay ExStart Exchange Loading Full Total
-----
1/1/2          0    0      0    0      0      0      0      1    1
Total          0    0      0    0      0      0      0      1    1
```

Showing OSPFv3 AF neighbors information for VRF red:

```
switch# show ospfv3-af ipv6 neighbors vrf red

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 2 VRF red
=====

Total Number of Neighbors: 1

Neighbor ID      Priority  State           Interface
-----
4.4.4.4          1        FULL/DR         1/1/2
Neighbor address fe80::7272:cfff:fe79:7510
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 routes

```
show ospfv3-af [<PROCESS-ID>] ipv6 routes [<PREFIX/LENGTH>]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows the OSPFv3 AF routing table information.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID that shows information from the OSPFv3 AF routing table for the particular OSPFv3 AF process. Range: 1 to 65535.
<PREFIX/LENGTH>	Specifies the IPv6 destination prefix showing information about a particular destination prefix. For example, 2010:bd9::/32.
all-vrfs	Select to show OSPFv3 AF routing table information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF routing table information:

```
switch# show ospfv3-af ipv6 routes
Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Routing Table
-----

Total Number of OSPFv3 AF Routes : 3

111::/64          (i) area:0.0.0.0
    directly attached to interface 1/1/1, cost 1 distance 110
2000::/64         (i) area:0.0.0.0
    directly attached to interface tunnell1, cost 100 distance 110
fd00::/64         (i) area:0.0.0.1
    directly attached to interface vlan10, cost 1 distance 110
```

Showing OSPFv3 AF routing table information for VRF red:

```
switch# show ospfv3-af ipv6 routes vrf red

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 2 VRF red, Routing Table
-----

Total Number of OSPFv3 AF Routes : 1

222::/64          (i) area:0.0.0.1
    directly attached to interface 1/1/2, cost 1 distance 110
```

Showing OSPFv3 AF routing table information for destination prefix fd00::/64:

```
switch# show ospfv3-af 1 ipv6 routes fd00::/64

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Routing Table for prefixes fd00::/64
-----

Total Number of OSPFv3 AF Routes : 1

fd00::/64          (i) area:0.0.0.1
    directly attached to interface vlan10, cost 1 distance 110
```

Showing OSPFv3 AF routing table information for destination prefix 2000::/64:

```
switch# show ospfv3-af 1 ipv6 routes 2000::/64

Codes: i - Intra-area route, I - Inter-area route
       E1 - External type-1, E2 - External type-2

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Routing Table for prefixes 2000::/64
-----

Total Number of OSPFv3 AF Routes : 1

2000::/64          (i) area:0.0.0.0
    directly attached to interface tunnel1, cost 100 distance 110
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 statistics

```
show ospfv3-af ipv6 [<PROCESS-ID>] statistics
[all-vrfs | vrf <VRF-NAME>]
```

Description

Shows OSPFv3 AF statistics.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID that shows information on the OSPFv3 AF SPF statistics for the particular OSPFv3 AF process. Range: 1 to 65535.
all-vrfs	Select to show OSPFv3 AF SPF statistics information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Showing OSPFv3 AF statistics information:

```
switch# show ospfv3-af ipv6 statistics

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Statistics (cleared 3h 2m 21s ago)
-----

Unknown Interface Drops      : 0
Unknown Virtual Interface Drops : 0
Bad IPv6 Header Length Drops : 0
Wrong OSPFv3 Version Drops   : 0
Bad Source IPv6 Drops        : 0
Resource Failure Drops        : 0
Bad Header Length Drops      : 0
Total Drops                   : 0
```

Showing OSPFv3 AF statistics information for VRF red:

```

switch# show ospfv3-af 2 ipv6 statistics vrf red

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 2 VRF red, Statistics (cleared 3h 2m 30s ago)
-----

Unknown Interface Drops           : 0
Unknown Virtual Interface Drops   : 0
Bad IPv6 Header Length Drops      : 0
Wrong OSPFv3 Version Drops        : 0
Bad Source IPv6 Drops             : 0
Resource Failure Drops            : 0
Bad Header Length Drops           : 0
Total Drops                       : 0

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 statistics interface

```

show ospfv3-af ipv6 [<PROCESS-ID>] statistics interface [<INTERFACE-NAME>| vlan <VLAN-ID>
| lag <LAG-ID> | loopback <LOOPBACK-ID> | tunnel <TUNNEL-ID>]
[all-vrfs | vrf <VRF-NAME>]

```

Description

Shows the OSPFv3 AF statistics for the enabled OSPFv3 AF interfaces.

Parameter	Description
<PROCESS-ID>	Specifies an OSPFv3 AF process ID to show OSPF-enabled interface statistics information on the specified OSPFv3 AF process. Range: 1 to 65535.
<INTERFACE-NAME>	Selects to show information only for the specified interface.
vlan <VLAN-ID>	Specifies the vlan interface name.
lag <LAG ID>	Specifies lag interface name.

Parameter	Description
loopback <LOOPBACK ID>	Specifies the vlan interface name.
tunnel <TUNNEL-ID>	Specifies the tunnel interface name.
all-vrfs	Select to show OSPF-enabled interface statistics information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Showing enabled OSPFv3 AF interfaces information for interface 1/1/1:

```
switch# show ospfv3-af ipv6 statistics interface 1/1/1

Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Interface 1/1/1 Statistics (cleared 3h 22m
18s ago)

=====
====

Tx Hello packets      : 1213          Rx Hello packets      : 1213
Tx Hello bytes        : 48516         Rx Hello bytes        : 48516
Tx DD packets         : 3             Rx DD packets         : 2
Tx DD bytes           : 164           Rx DD bytes           : 136
Tx LS request packets : 1             Rx LS request packets : 1
Tx LS request bytes   : 64            Rx LS request bytes   : 64
Tx LS update packets  : 22            Rx LS update packets  : 22
Tx LS update bytes    : 1520          Rx LS update bytes    : 1844
Tx LS ack packets     : 21            Rx LS ack packets     : 20
Tx LS ack bytes       : 976           Rx LS ack bytes       : 800

Total IPsec packets processed : 10
Total IPsec bytes processed   : 6400
Total Number of State Changes : 3
Number of LSAs                : 2
LSA Checksum Sum              : 21758

Total OSPFv3-AF Packets Discarded: 0
-----

Reason                      Packets Dropped
-----
Invalid Type                 0
Invalid Length               0
Invalid Version              0
Bad or Unknown Source        0
Area Mismatch                0
Self-originated              0
Duplicate Router ID          0
Interface Standby            0
Total Hello Packets Dropped  0
  Hello Interval Mismatch    0
  Dead Interval Mismatch     0
  Options Mismatch           0
  MTU Mismatch               0
```



```

Neighbor Ignored          0
Resource Failures         0
Bad LSA Length            0
Others                    0
IPsec Authentication Errors 0

```

```
Total LSAs Ignored : 0
```

```

-----
Bad Type      : 0
Bad Length    : 0
Invalid Data  : 0
Invalid Checksum : 0

```

Showing enabled OSPFv3 AF interfaces information for tunnel interface:

```
switch# show ospfv3-af ipv6 statistics interface tunnel1
```

```
Address-family : IPv6 Unicast
```

```
OSPFv3 AF Process ID 1 VRF default, Interface tunnel1 Statistics (cleared 0h16m32s ago)
```

```
=====
===
```

Tx Hello packets	: 100	Rx Hello packets	: 75
Tx Hello bytes	: 3900	Rx Hello bytes	: 3000
Tx DD packets	: 2	Rx DD packets	: 2
Tx DD bytes	: 136	Rx DD bytes	: 116
Tx LS request packets	: 1	Rx LS request packets	: 1
Tx LS request bytes	: 52	Rx LS request bytes	: 64
Tx LS update packets	: 3	Rx LS update packets	: 5
Tx LS update bytes	: 388	Rx LS update bytes	: 464
Tx LS ack packets	: 4	Rx LS ack packets	: 3
Tx LS ack bytes	: 244	Rx LS ack bytes	: 208

```

Total IPsec packets processed : 0
Total IPsec bytes processed   : 0
Total Number of State Changes : 2
Number of LSAs                : 2
LSA Checksum Sum              : 76646

```

```
Total OSPFv3-AF Packets Discarded: 0
```

Reason	Packets Dropped
Invalid Type	0
Invalid Length	0
Invalid Version	0
Bad or Unknown Source	0
Area Mismatch	0
Self-originated	0
Duplicate Router ID	0
Interface Standby	0
Total Hello Packets Dropped	0
Hello Interval Mismatch	0
Dead Interval Mismatch	0
Options Mismatch	0
MTU Mismatch	0

```
Neighbor Ignored          0
Resource Failures         0
Bad LSA Length            0
Others                    0
IPsec Authentication Errors 0
IPsec ESP Errors          0

Total LSAs Ignored : 0
-----
Bad Type               : 0
Bad Length             : 0
Invalid Data           : 0
Invalid Checksum       : 0
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ospfv3-af ipv6 virtual-links

```
show ospfv3-af [<PROCESS-ID>] ipv6 virtual-links [brief]
[all-vrfs | vrf <VRF-NAME>]
```

Description

Displays the current state and parameters of the OSPFv3 AF virtual links.

Parameter	Description
<PROCESS-ID>	Enter an OSPFv3 AF process ID to display information on the OSPFv3 AF virtual links for the particular OSPFv3 AF process. Range: 1 to 65535.
brief	Select to display brief overview information for the OSPFv3 AF virtual links.
all-vrfs	Select to display OSPFv3 AF virtual links information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Show OSPFv3 AF virtual links information:

```

switch# show ospfv3-af ipv6 virtual-links

Address-family : IPv6 Unicast
-----

Virtual link to router 40.40.40.40 is up
-----

VRF                : default                Process                : 21
Transit area       : 0.0.0.1                Authentication        : No
Hello Interval     : 10                     Dead Interval         : 40
Transit Delay      : 1                     Retransmit Interval   : 5
Number of Link LSAs : 0                     Checksum Sum          : 0
Authentication     : No
Number of State Changes : 4

```

Show OSPFv3 AF virtual links information with IPsec AH authentication:

```

switch# show ospfv3-af ipv6 virtual-links

Address-family : IPv6 Unicast
-----

Virtual link to router 40.40.40.40 is up
-----

VRF                : default                Process                : 21
Transit area       : 0.0.0.1                Authentication        : No
Hello Interval     : 10                     Dead Interval         : 40
Transit Delay      : 1                     Retransmit Interval   : 5
Number of Link LSAs : 0                     Checksum Sum          : 0
AH Authentication  : MD5 SPI: 1234
Number of State Changes : 4

```

Show OSPFv3 AF virtual links information with IPsec ESP authentication:

```

switch# show ospfv3-af ipv6 virtual-links

Address-family : IPv6 Unicast
-----

Virtual link to router 40.40.40.40 is up
-----

VRF                : default                Process                : 21
Transit area       : 0.0.0.1                Authentication        : No
Hello Interval     : 10                     Dead Interval         : 40
Transit Delay      : 1                     Retransmit Interval   : 5
Number of Link LSAs : 0                     Checksum Sum          : 0
ESP Authentication : SHA1 Encryption: NULL SPI: 1234
Number of State Changes : 4

```

Show brief overview information for OSPFv3 AF virtual links:

```

switch# show ospfv3-af ipv6 virtual-links brief

Address-family : IPv6 Unicast

```

```

-----
OSPFv3 AF Process ID 1 VRF default
=====

Total Number of Virtual Links: 1

Neighbor-ID      Transit-Area      Status
-----
2.1.1.2          0.0.0.1          down

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config

show running-config

Description

This command shows the configurations for all the protocols along with OSPFv3 AF.

Example

```

switch# show running-config
Current configuration:
!
!Version ArubaOS-CX genericx86-64.01.01.000X
!Schema version 0.1.8
vrf blue
vrf green
vrf red
led locator on
!
!
!
!
!
!
!
vlan 1,10

```

```

interface 1/1/1
  no shutdown
  ip address 1.1.1.1/24
  ipv6 address 111::1/64
  ip ospf 1 area 0.0.0.0
  ospfv3-af 1 ipv4 area 0.0.0.0
  ospfv3-af ipv4 authentication ipsec spi 300 sha1 ciphertext
  AQBapXl/Ow3jK2zC6WCov3mGwmvDQ02L9WKRTxVPtSyXpUNqBQAAACoBmj2c
interface 1/1/2
  no shutdown
  vrf attach red
  ip address 2.2.2.2/24
  ipv6 address 222::2/64
  ip ospf 2 area 0.0.0.1
  ospfv3-af 1 ipv4 area 0.0.0.1
  ospfv3-af ipv4 authentication ipsec spi 300 md5 ciphertext
  AQBapYH+i/6HV2w+yyJCb45XhHPffLNIt876Mh9EMRyf0XgwBAAAAGE/tKs=
interface 1/1/3
  no shutdown
  ip address 3.3.3.1/24
  ipv6 address 333::3/64
  ospfv3-af 1 ipv6 area 0.0.0.0 instance 1
  no ospfv3-af ipv6 passive
  ospfv3-af 1 ipv4 area 0.0.0.0 instance 65
interface 1/1/4
  no shutdown
  ipv6 address 1000::1/64
interface tunnel 1 mode ip 6in6
  no shutdown
  source ipv6 1000::1
  destination ipv6 1000::2
  ipv6 address 2000::1/64
  ospfv3-af 1 ipv4 area 0.0.0.0
  ospfv3-af ipv4 passive
  ospfv3-af ipv4 hello-interval 22
  ospfv3-af ipv4 dead-interval 88
  ospfv3-af ipv4 transit-delay 44
  ospfv3-af ipv4 priority 88
  ospfv3-af ipv4 cost 8
  ospfv3-af ipv4 network point-to-point
  ospfv3-af ipv4 shutdown
interface vlan10
  ip address 10.1.1.1/24
  ipv6 address fd00::1/64
  ip ospf 1 area 0.0.0.0
  ospfv3-af 1 ipv4 area 0.0.0.1
  ospfv3-af ipv4 encryption ipsec spi 401 sha1 ciphertext
  AQBapd+HuD8Y4kMJkh5dFzG6OTBvW4iY+ueK4xpETxZPsZlFDgAAAE3pkLmvMCtdFk2zz/LS
  aes ciphertext
  AQBapbPnk0Kl9giahf2dWGRHcU+6mTFiWzfxeWUXuWGYQ4teIgAAAOG7kcVrkrKV754nX+Li1ZDYPHG5xs
  apOnyZJMv7cfHEctA=
  ospfv3-af 1 ipv6 area 0.0.0.1
  ospfv3-af ipv4 encryption ipsec spi 401 sha1 ciphertext
  AQBapd+HuD8Y4kMJkh5dFzG6OTBvW4iY+ueK4xpETxZPsZlFDgAAAE3pkLmvMCtdFk2zz/LS
  aes ciphertext
  AQBapbPnk0Kl9giahf2dWGRHcU+6mTFiWzfxeWUXuWGYQ4teIgAAAOG7kcVrkrKV754nX+Li1ZDYPHG5xs
  apOnyZJMv7cfHEctA=
interface loopback 2
  ipv6 address 99::1/64
  ospfv3-af 1 ipv4 area 0.0.0.0
router ospfv3-af 1
  router-id 1.1.1.1

```

```

reference-bandwidth 4000
address-family ipv4 unicast
    router-id 2.2.2.1
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2
    area 0.0.0.3
    distribute-list prefix list2 in
    redistribute static
    reference-bandwidth 4000
    active-backbone stub-default-route
exit-address-family
address-family ipv6 unicast
    router-id 2.2.2.2
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2
    area 0.0.0.3
    distribute-list prefix list2 in
    passive-interface default
    redistribute static
    reference-bandwidth 4000
    active-backbone stub-default-route
    area 0.0.0.1 virtual-link 1.1.1.1
        hello-interval 15
        dead-interval 60
        authentication ipsec spi 256 md5 ciphertext
AQBapYH+i/6HV2w+yyJCb45XhHPFFLNIt876Mh9EMRyf0XgwBAAAAGE/tKs=
    exit
    area 0.0.0.1 authentication ipsec spi 256 md5 ciphertext
AQBapYH+i/6HV2w+yyJCb45XhHPFFLNIt876Mh9EMRyf0XgwBAAAAGE/tKs=
    area 0.0.0.2 virtual-link 2.2.2.2
        encryption ipsec spi 3456 md5 ciphertext
AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVMiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8 null
    exit
    area 0.0.0.3 virtual-link 3.3.3.3
        encryption ipsec spi 5678 sha1 ciphertext
AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVMiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8 des
ciphertext AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVMiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8
    exit
exit-address-family
router ospfv3-af 2
    router-id 1.1.1.3
    distance 88
    max-metric router-lsa
    throttle spf start-time 100 hold-time 1000 max-wait-time 10000
    address-family ipv4 unicast
        router-id 1.1.1.3
        distance 88
        area 0.0.0.0
        area 0.0.0.1
        passive-interface default
        redistribute ospfv3-af 1 route-map ospfv3_af4_routes
        max-metric router-lsa
        throttle spf start-time 100 hold-time 1000 max-wait-time 10000
        area 0.0.0.1 encryption ipsec spi 400 md5 ciphertext
AQBapfwg9p/z+rRS1mhk9jXzbOFBd82j2OSvEbAbI2f4KL+ADAAAAL3hhFDJlUbBwulfvA==
des ciphertext
AQBapfTQ8jUL+zbNyX9ZKOF8Lc5iR6dF543pwK2egyCWSWkkEgAAAE0etJaie2d/i2XF8pKkRpQvpw==
    exit-address-family
    address-family ipv6 unicast
        router-id 1.1.1.4

```

```

distance 88
area 0.0.0.0
area 0.0.0.1
passive-interface default
redistribute ospfv3-af 1 route-map ospfv3_af6_routes
max-metric router-lsa
throttle spf start-time 100 hold-time 1000 max-wait-time 10000
area 0.0.0.1 encryption ipsec spi 400 md5 ciphertext
AQBapfwg9p/z+rRS1mhk9jXzbOFBd82j2OSvEbAbI2f4KL+ADAAAAL3hhFDJlUbBwulfvA==
des ciphertext
AQBapfTQ8jUL+zbNyX9ZKOF8Lc5iR6dF543pwK2egyCWSWkkEgAAAE0etJaie2d/i2XF8pKkRpQvpw==
exit-address-family
router ospfv3-af 1 vrf red
reference-bandwidth 40000
graceful-restart restart-interval 88
no graceful-restart helper
distance intra-area 34 inter-area 66 external 3
address-family ipv4 unicast
area 0.0.0.1
redistribute ospf 2
redistribute ospfv3-af 2
reference-bandwidth 40000
graceful-restart restart-interval 88
no graceful-restart helper
distance intra-area 34 inter-area 66 external 3
exit-address-family
address-family ipv6 unicast
area 0.0.0.1
redistribute ospfv3 2
redistribute ospfv3-af 2
reference-bandwidth 40000
graceful-restart restart-interval 88
max-metric router-lsa include-stub
graceful-restart restart-interval 88
no graceful-restart helper
graceful-restart ignore-lost-interface
distance intra-area 34 inter-area 66
address-family ipv4 unicast
router-id 1.1.1.8
area 0.0.0.1
max-metric router-lsa include-stub
graceful-restart restart-interval 88
no graceful-restart helper
graceful-restart ignore-lost-interface
distance intra-area 34 inter-area 66
exit-address-family
address-family ipv6 unicast
router-id 1.1.1.9
area 0.0.0.1
graceful-restart restart-interval 88
no graceful-restart helper strict-lsa-check
max-metric router-lsa include-stub
distance intra-area 34 inter-area 66
exit-address-family
router ospfv3-af 1 vrf blue
graceful-restart restart-interval 99
no graceful-restart helper
max-metric router-lsa on-startup 100
address-family ipv4 unicast
graceful-restart restart-interval 99
no graceful-restart helper
area 0.0.0.0

```

```

        max-metric router-lsa on-startup 100
    exit-address-family
    address-family ipv6 unicast
        graceful-restart restart-interval 99
        no graceful-restart helper
        area 0.0.0.0
        max-metric router-lsa on-startup 100
    exit-address-family
router ospfv3-af 1 vrf green
    max-metric router-lsa include-stub on-startup 100
    address-family ipv4 unicast
        area 0.0.0.0
        max-metric router-lsa include-stub on-startup 100
    exit-address-family
    address-family ipv6 unicast
        area 0.0.0.0
        max-metric router-lsa include-stub on-startup 100
    exit-address-family
switch#

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config all

```
show running-config all
```

Description

Displays the current running configuration, including default values for all protocols such as OSPFv3 AF.

Examples

Showing running-config without default values:

```

switch# show running-config
Current configuration:
!
!Version ArubaOS-CX Virtual.10.05.0001BC-26-g94067ba
!export-password: default
led locator on

```



```

vrf blue
vrf green
vrf red
!
!
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/1
    no shutdown
    ip address 1.1.1.1/24
    ipv6 address 111::1/64
    ipv6 address 99::1/64
    ospfv3-af 1 ipv4 area 0.0.0.0
interface 1/1/2
    no shutdown
interface loopback 2
    ipv6 address 929::1/64
    ospfv3-af 1 ipv4 area 0.0.0.0
interface loopback 3
    ipv6 address 123::1/64
    ospfv3-af 1 ipv4 area 0.0.0.0
    ospfv3-af 1 ipv6 area 0.0.0.0
!
!
!
!
!
router ospfv3-af 1 vrf blue
    max-metric router-lsa on-startup 100
    address-family ipv4 unicast
        distribute-list prefix list2 in
        max-metric router-lsa on-startup 100
        active-backbone stub-default-route
        area 0.0.0.0
    exit-address-family
    address-family ipv6 unicast
        distribute-list prefix list2 in
        max-metric router-lsa on-startup 100
        active-backbone stub-default-route
        area 0.0.0.0
    exit-address-family
router ospfv3-af 1
    router-id 1.1.1.1
    reference-bandwidth 4000
    address-family ipv4 unicast
        router-id 1.1.1.2
        reference-bandwidth 4000
        redistribute host-routes
        redistribute static
        area 0.0.0.0
        area 0.0.0.1
    exit-address-family
    address-family ipv6 unicast
        router-id 1.1.1.3
        reference-bandwidth 4000
        redistribute host-routes
        redistribute static

```

```

    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.1 virtual-link 1.1.1.2
        dead-interval 60
        hello-interval 15
        authentication ipsec spi 256 md5 ciphertext
        AQBapYH+i/6HV2w+yyJCb45XhHPFFLNIt876Mh9EMRyf0XgwBAAAAGE/tKs=
        exit
    area 0.0.0.2
    area 0.0.0.2 virtual-link 2.2.2.2
        encryption ipsec spi 3456 md5 ciphertext
        AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVmiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8 null
        exit
    area 0.0.0.3
    area 0.0.0.3 virtual-link 3.3.3.3
        encryption ipsec spi 5678 sha1 ciphertext
        AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVmiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8 des
        ciphertext AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVmiduKtDwIP1jbCCxZCAAAAEe+
        Xod/lZX8
        exit
    exit-address-family
router ospfv3-af 2
    router-id 1.1.1.3
    max-metric router-lsa
    address-family ipv4 unicast
        router-id 1.1.1.4
        max-metric router-lsa
        area 0.0.0.0
        area 0.0.0.1
        area 0.0.0.1 encryption ipsec spi 400 md5 ciphertext

AQBapfwg9p/z+rRS1mhk9jXzbOFBd82j2OSvEbAbI2f4KL+ADAAAAL3hhFDJlUbBwulfvA==des
ciphertext
AQBapfTQ8jUL+zbNyX9ZKOF8Lc5iR6dF543pwK2egyCWSWkkEgAAAE0etJaie2d/
i2XF8pKkRpQvpw==
    exit-address-family
    address-family ipv6 unicast
        router-id 1.1.1.5
        max-metric router-lsa
        area 0.0.0.0
        area 0.0.0.1
        area 0.0.0.1 encryption ipsec spi 400 md5 ciphertext

AQBapfwg9p/z+rRS1mhk9jXzbOFBd82j2OSvEbAbI2f4KL+ADAAAAL3hhFDJlUbBwulfvA==des
ciphertext
AQBapfTQ8jUL+zbNyX9ZKOF8Lc5iR6dF543pwK2egyCWSWkkEgAAAE0etJaie2d/
i2XF8pKkRpQvpw==
    exit-address-family
router ospfv3-af 1 vrf green
    max-metric router-lsa include-stub on-startup 100
    address-family ipv4 unicast
        max-metric router-lsa include-stub on-startup 100
        area 0.0.0.0
    exit-address-family
    address-family ipv6 unicast
        max-metric router-lsa include-stub on-startup 100
        area 0.0.0.0
    exit-address-family
router ospfv3-af 1 vrf red
    reference-bandwidth 40000
    address-family ipv4 unicast
        reference-bandwidth 40000

```

```

        redistribute ospfv3 2
        area 0.0.0.1
    exit-address-family
    address-family ipv6 unicast
        reference-bandwidth 40000
        redistribute ospfv3 2
        area 0.0.0.1
    exit-address-family
router ospfv3-af 2 vrf red
    router-id 1.1.1.7
    max-metric router-lsa include-stub
    address-family ipv4 unicast
        router-id 1.1.1.7
        max-metric router-lsa include-stub
        area 0.0.0.1
    exit-address-family
    address-family ipv6 unicast
        router-id 1.1.1.7
        max-metric router-lsa include-stub
        area 0.0.0.1
    exit-address-family
https-server vrf mgmt

```

Showing running-config with default values:

```

switch# show running-config all
Current configuration:
!
!
!
interface 1/1/1
    no shutdown
    mtu 1500
    qos trust none
    apply qos schedule-profile factory-default
    lldp transmit
    lldp receive
    lldp med poe
    no lldp med poe priority-override
    lldp dot3 poe
    lldp dot3 macphy
    lldp med network-policy
    lldp med capability
    lldp med topology-trap
    cdp
    sflow
    routing
    vrf attach default
    ip mtu 1500
    ip address 1.1.1.1/24
    ipv6 address 111::1/64 tag 0
    ipv6 address 99::1/64 tag 0
    no ip urpf-check
    ipv6 nd mtu 1500
    no ip proxy-arp
    ipv6 nd dad attempts 1
    ipv6 nd hop-limit 64
    ipv6 nd ns-interval 1000
    ipv6 nd ra min-interval 200
    ipv6 nd ra max-interval 600
    ipv6 nd ra lifetime 1800

```

```

ipv6 nd ra reachable-time 0
no ipv6 address autoconfig
ipv6 nd ra retrans-timer 0
no ipv6 nd ra managed-config-flag
no ipv6 nd ra other-config-flag
ipv6 nd suppress-ra
ipv6 nd router-preference medium
no ip irdp
ip irdp multicast
ip irdp minadvertinterval 450
ip irdp maxadvertinterval 600
ip irdp holdtime 1800
ip irdp preference 0
arp timeout 1800
ipv6 neighbor timeout 1800
power-over-ethernet
no power-over-ethernet pre-std-detect
power-over-ethernet priority low
power-over-ethernet allocate-by usage
power-over-ethernet assigned-class 4
ospfv3-af 1 ipv4 area 0.0.0.0
ospfv3-af ipv4 dead-interval 40
ospfv3-af ipv4 hello-interval 10
ospfv3-af ipv4 retransmit-interval 5
ospfv3-af ipv4 transit-delay 1
ospfv3-af ipv4 priority 1
ospfv3-af ipv4 cost 4
ospfv3-af ipv4 network broadcast
!
!
!
interface loopback 2
  vrf attach default
  ipv6 address 929::1/64 tag 0
  no ip urpf-check
  arp timeout 1800
  ipv6 neighbor timeout 1800
  ospfv3-af 1 ipv4 area 0.0.0.0
  ospfv3-af ipv4 dead-interval 40
  ospfv3-af ipv4 hello-interval 10
  ospfv3-af ipv4 retransmit-interval 5
  ospfv3-af ipv4 transit-delay 1
  ospfv3-af ipv4 priority 1
  ospfv3-af ipv4 network broadcast
!
!
!
interface loopback 3
  vrf attach default
  ipv6 address 123::1/64 tag 0
  no ip urpf-check
  arp timeout 1800
  ipv6 neighbor timeout 1800
  ospfv3-af 1 ipv4 area 0.0.0.0
  ospfv3-af ipv4 dead-interval 40
  ospfv3-af ipv4 hello-interval 10
  ospfv3-af ipv4 retransmit-interval 5
  ospfv3-af ipv4 transit-delay 1
  ospfv3-af ipv4 priority 1
  ospfv3-af ipv4 network broadcast
  ospfv3-af 1 ipv6 area 0.0.0.0
  ospfv3-af ipv6 dead-interval 40

```

```

ospfv3-af ipv6 hello-interval 10
ospfv3-af ipv6 retransmit-interval 5
ospfv3-af ipv6 transit-delay 1
ospfv3-af ipv6 priority 1
ospfv3-af ipv6 network broadcast
!
!
!
router ospfv3-af 1 vrf blue
  enable
  reference-bandwidth 100000
  max-metric router-lsa on-startup 100
  timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
  timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
  timers lsa-arrival 1000
  graceful-restart restart-interval 120
  distance 110
  address-family ipv4 unicast
    enable
    reference-bandwidth 100000
    max-metric router-lsa on-startup 100
    maximum-paths 4
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
    timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
    timers lsa-arrival 1000
    graceful-restart restart-interval 120
    default-metric 25
    distance 110
    active-backbone stub-default-route
    area 0.0.0.0
    area 0.0.0.0 default-metric 1
  exit-address-family
  address-family ipv6 unicast
    enable
    reference-bandwidth 100000
    max-metric router-lsa on-startup 100
    maximum-paths 4
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
    timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
    timers lsa-arrival 1000
    graceful-restart restart-interval 120
    default-metric 25
    distance 110
    active-backbone stub-default-route
    area 0.0.0.0
    area 0.0.0.0 default-metric 1
  exit-address-family
router ospfv3-af 1 vrf default
  enable
  router-id 1.1.1.1
  reference-bandwidth 4000
  timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
  timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
  timers lsa-arrival 1000
  graceful-restart restart-interval 120
  distance 110
  address-family ipv4 unicast
    enable
    router-id 1.1.1.1
    reference-bandwidth 4000
    maximum-paths 4
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000

```

```

timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
default-metric 25
distance 110
redistribute static
no active-backbone stub-default-route
area 0.0.0.0
area 0.0.0.0 default-metric 1
area 0.0.0.1
area 0.0.0.1 default-metric 1
area 0.0.0.2
area 0.0.0.2 default-metric 1
area 0.0.0.3
area 0.0.0.3 default-metric 1
exit-address-family
address-family ipv6 unicast
enable
router-id 1.1.1.1
reference-bandwidth 4000
maximum-paths 4
timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
default-metric 25
distance 110
redistribute static
no active-backbone stub-default-route
area 0.0.0.0
area 0.0.0.0 default-metric 1
area 0.0.0.1
area 0.0.0.1 default-metric 1
area 0.0.0.1 virtual-link 1.1.1.2
    dead-interval 60
    hello-interval 15
    retransmit-interval 5
    transit-delay 1
    authentication ipsec spi 256 md5 ciphertext
    AQBapYH+i/6HV2w+yyJCb45XhHPFFlNIt876Mh9EMRyf0XgwBAAAAGE/tKs=
    exit
area 0.0.0.2
area 0.0.0.2 default-metric 1
area 0.0.0.2 virtual-link 2.2.2.2
    dead-interval 40
    hello-interval 10
    retransmit-interval 5
    transit-delay 1
    encryption ipsec spi 3456 md5 ciphertext
    AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVmiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8 null
    exit
area 0.0.0.3
area 0.0.0.3 default-metric 1
area 0.0.0.3 virtual-link 3.3.3.3
    dead-interval 40
    hello-interval 10
    retransmit-interval 5
    transit-delay 1
    encryption ipsec spi 5678 sha1 ciphertext
    AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVmiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8 des
    ciphertext
AQBapVuqYeTJuT8/BoIlC2z4MxuT3VVmiduKtDwIP1jbCCxZCAAAAEe+Xod/lZX8

```

```

        exit
    exit-address-family
router ospfv3-af 2 vrf default
    enable
    router-id 1.1.1.3
    reference-bandwidth 100000
    max-metric router-lsa
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
    timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
    timers lsa-arrival 1000
    graceful-restart restart-interval 120
    distance 110
    address-family ipv4 unicast
        enable
        router-id 1.1.1.3
        reference-bandwidth 100000
        max-metric router-lsa
        maximum-paths 4
        timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
        timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
        timers lsa-arrival 1000
        graceful-restart restart-interval 120
        default-metric 25
        distance 110
        no active-backbone stub-default-route
        area 0.0.0.0
        area 0.0.0.0 default-metric 1
        area 0.0.0.1
        area 0.0.0.1 encryption ipsec spi 400 md5 ciphertext

AQBapfwg9p/z+rRS1mhk9jXzbOFBd82j2OSvEbAbI2f4KL+ADAAAAL3hhFDJlUbBwulfvA==des
ciphertext
AQBapfTQ8jUL+zbNyX9ZKOF8Lc5iR6dF543pwK2egyCWSWkkEgAAAE0etJaie2d/
i2XF8pKkRpQvpw==
    area 0.0.0.1 default-metric 1
    exit-address-family
    address-family ipv6 unicast
        enable
        router-id 1.1.1.3
        reference-bandwidth 100000
        max-metric router-lsa
        maximum-paths 4
        timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
        timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
        timers lsa-arrival 1000
        graceful-restart restart-interval 120
        default-metric 25
        distance 110
        no active-backbone stub-default-route
        area 0.0.0.0
        area 0.0.0.0 default-metric 1
        area 0.0.0.1
        area 0.0.0.1 encryption ipsec spi 400 md5 ciphertext

AQBapfwg9p/z+rRS1mhk9jXzbOFBd82j2OSvEbAbI2f4KL+ADAAAAL3hhFDJlUbBwulfvA==des
ciphertext
AQBapfTQ8jUL+zbNyX9ZKOF8Lc5iR6dF543pwK2egyCWSWkkEgAAAE0etJaie2d/
i2XF8pKkRpQvpw==
    area 0.0.0.1 default-metric 1
    exit-address-family
router ospfv3-af 1 vrf green
    enable

```

```

reference-bandwidth 100000
max-metric router-lsa include-stub on-startup 100
timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
distance 110
address-family ipv4 unicast
    enable
    reference-bandwidth 100000
    max-metric router-lsa include-stub on-startup 100
    maximum-paths 4
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
    timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
    timers lsa-arrival 1000
    graceful-restart restart-interval 120
    default-metric 25
    distance 110
    no active-backbone stub-default-route
    area 0.0.0.0
    area 0.0.0.0 default-metric 1
exit-address-family
address-family ipv6 unicast
    enable
    reference-bandwidth 100000
    max-metric router-lsa include-stub on-startup 100
    maximum-paths 4
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
    timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
    timers lsa-arrival 1000
    graceful-restart restart-interval 120
    default-metric 25
    distance 110
    no active-backbone stub-default-route
    area 0.0.0.0
    area 0.0.0.0 default-metric 1
exit-address-family
router ospfv3 af 1 vrf red
    enable
    reference-bandwidth 40000
    timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
    timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
    timers lsa-arrival 1000
    graceful-restart restart-interval 120
    distance 110
    address-family ipv4 unicast
        enable
        reference-bandwidth 40000
        maximum-paths 4
        timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
        timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
        timers lsa-arrival 1000
        graceful-restart restart-interval 120
        default-metric 25
        distance 110
        redistribute ospfv3 2
        no active-backbone stub-default-route
        area 0.0.0.1
        area 0.0.0.1 default-metric 1
    exit-address-family
    address-family ipv6 unicast
        enable

```



```

reference-bandwidth 40000
maximum-paths 4
timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
default-metric 25
distance 110
redistribute ospfv3 2
no active-backbone stub-default-route
area 0.0.0.1
area 0.0.0.1 default-metric 1
exit-address-family
router ospfv3-af 2 vrf red
enable
router-id 1.1.1.7
reference-bandwidth 100000
max-metric router-lsa include-stub
timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
distance 110
address-family ipv4 unicast
enable
router-id 1.1.1.7
reference-bandwidth 100000
max-metric router-lsa include-stub
maximum-paths 4
timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
default-metric 25
distance 110
no active-backbone stub-default-route
area 0.0.0.1
area 0.0.0.1 default-metric 1
exit-address-family
address-family ipv6 unicast
enable
router-id 1.1.1.7
reference-bandwidth 100000
max-metric router-lsa include-stub
maximum-paths 4
timers throttle spf start-time 200 hold-time 1000 max-wait-time 5000
timers throttle lsa start-time 5000 hold-time 0 max-wait-time 0
timers lsa-arrival 1000
graceful-restart restart-interval 120
default-metric 25
distance 110
no active-backbone stub-default-route
area 0.0.0.1
area 0.0.0.1 default-metric 1
exit-address-family
!
!
!
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tech ospfv3-af

show tech ospfv3-af [local-file]

Description

Shows the output of the following OSPFv3 AF commands:

- `show ospfv3-af all vrfs`
- `show ospfv3-af interface all-vrfs`
- `show ospfv3-af neighbors detail all-vrfs`
- `show ospfv3-af neighbors summary all-vrfs`
- `show ospfv3-af route all-vrfs`
- `show ospfv3-af statistics all-vrfs`
- `show ospfv3-af statistics interface all-vrfs`
- `show ospfv3-af border-routers all-vrfs`
- `show ospfv3-af lsdb all-vrfs database-summary`
- `show ospfv3-af virtual-links all-vrfs`

Parameter	Description
local-file	Captures the command output into a local file. Optional.

Examples

```
switch(config-if)# show tech ospfv3-af
=====
Show Tech executed on Tue Sep 12 09:42:42 2017
=====
[Begin] Feature ospfv3-af
=====

*****
Command : show ospfv3-af ipv6 neighbor summary all-vrfs
*****
Address-family : IPv6 Unicast
-----
```

OSPFv3 AF Process ID 1 VRF default, Neighbor Summary

=====

Interface	Down	Attempt	Init	TwoWay	ExStart	Exchange	Loading	Full	Total
1/1/1	0	0	0	0	0	0	0	1	1
Total	0	0	0	0	0	0	0	1	1

OSPFv3 AF Process ID 1 VRF red, Neighbor Summary

=====

Interface	Down	Attempt	Init	TwoWay	ExStart	Exchange	Loading	Full	Total
1/1/2	0	0	0	0	0	0	0	1	1
Total	0	0	0	0	0	0	0	1	1

Command : show ospfv3-af ipv6 statistics all-vrfs

Address-family : IPv6 Unicast

OSPFv3 AF Process ID 1 VRF default, Statistics (cleared 0h 4m 46s ago)

```
Unknown Interface Drops      : 0
Unknown Virtual Interface Drops : 0
Bad IPv6 Header Length Drops : 0
Wrong OSPFv3 Version Drops   : 0
Bad Source IPv6 Drops        : 0
Resource Failure Drops       : 0
Bad Header Length Drops      : 0
Total Drops                  : 0
```

OSPFv3 AF Process ID 2 VRF red, Statistics (cleared 0h 4m 45s ago)

```
Unknown Interface Drops      : 0
Unknown Virtual Interface Drops : 0
Bad IPv6 Header Length Drops : 0
Wrong OSPFv3 Version Drops   : 0
Bad Source IPv6 Drops        : 0
Resource Failure Drops       : 0
Bad Header Length Drops      : 0
Total Drops                  : 0
```

Command : show ospfv3-af ipv6 neighbor detail all-vrfs

Address-family : IPv6 Unicast

Neighbor 3.3.3.3, Interface address fe80::7272:cfff:fec6:6e6c

```
Process ID 1 VRF default, in Area 0.0.0.0 via Interface 1/1/1
  State is FULL, Neighbor priority is 1
  DR is 3.3.3.3, BDR is 1.1.1.3
  Options is 0x13
  Dead timer due in 00:00:34
  Retransmission queue length 0
```

Neighbor 4.4.4.4, Interface address fe80::7272:cfff:fec6:6e6c

Process ID 2 VRF red, in Area 0.0.0.1 via Interface 1/1/2
State is FULL, Neighbor priority is 1
DR is 4.4.4.4, BDR is 1.1.1.7
Options is 0x13
Dead timer due in 00:00:35
Retransmission queue length 0

Command : show ospfv3-af ipv6 route all-vrfs

Address-family : IPv6 Unicast

Codes: i - Intra-area route, I - Inter-area route
E1 - External type-1, E2 - External type-2

OSPFv3 AF Process ID 1 VRF default, Routing Table

Total Number of OSPFv3 Routes : 2

111::/64 (i) area:0.0.0.0
directly attached to interface 1/1/1, cost 1 distance 110
fd00::/64 (i) area:0.0.0.1
directly attached to interface vlan10, cost 1 distance 110

OSPFv3 AF Process ID 2 VRF red, Routing Table

Total Number of OSPFv3 Routes : 1

222::/64 (i) area:0.0.0.1
directly attached to interface 1/1/2, cost 1 distance 110

Command : show ospfv3-af ipv6 all-vrfs

Address-family : IPv6 Unicast

Routing Process 1 with ID: 1.1.1.3 VRF default

Graceful-restart is configured
Restart Interval: 120, State: inactive
Last Graceful Restart Exit Status: none
Maximum Paths to Destination: 4
Number of external LSAs 0, checksum sum 0
Number of areas is: 2, 2 normal, 0 stub
Number of active areas is: 2, 2 normal, 0 stub
Area (0.0.0.0) (Active)
Interfaces in this Area: 1 Active Interfaces: 1
Passive Interfaces: 0 Loopback Interfaces: 0
SPF calculation has run 5 times
Number of LSAs: 5, checksum sum 138261
Area (0.0.0.1) (Active)
Interfaces in this Area: 1 Active Interfaces: 1

```

Passive Interfaces: 0 Loopback Interfaces: 0
SPF calculation has run 5 times
Area ranges:
  fd00::1/64, inter-area, no-advertise
Number of LSAs: 4, checksum sum 85028

Routing Process 2 with ID: 1.1.1.7 VRF red
-----

Graceful-restart is configured
Restart Interval: 120, State: inactive
Last Graceful Restart Exit Status: none
Maximum Paths to Destination: 4
Number of external LSAs 0, checksum sum 0
Number of areas is: 1, 1 normal, 0 stub
Number of active areas is: 1, 1 normal, 0 stub
Area (0.0.0.1) (Active)
  Interfaces in this Area: 1 Active Interfaces: 1
  Passive Interfaces: 0 Loopback Interfaces: 0
  SPF calculation has run 4 times
  Number of LSAs: 4, checksum sum 149947

*****
Command : show ospfv3-af ipv6 interface all-vrfs
*****
Address-family : IPv6 Unicast
-----

Interface 1/1/1 is up, Line Protocol is up
-----

IPv6 address fe80::7272:cfff:fea7:c8fa
Process ID 1 VRF default, Area 0.0.0.0
  State Backup-dr, Status up, Network type Broadcast, cost 1
  Transit delay 1 sec, Router priority 1
  Designated Router ID: 3.3.3.3
  Backup Designated Router ID: 1.1.1.3
  Timer Intervals: Hello 10, Dead 40, Retransmit 5
  Number of Link LSAs: 2, checksum sum 60947

Interface 1/1/2 is up, Line Protocol is up
-----

IPv6 address fe80::7272:cfff:fea7:c8fa
Process ID 2 VRF red, Area 0.0.0.1
  State Backup-dr, Status up, Network type Broadcast, cost 1
  Transit delay 1 sec, Router priority 1
  Designated Router ID: 4.4.4.4
  Backup Designated Router ID: 1.1.1.7
  Timer Intervals: Hello 10, Dead 40, Retransmit 5
  Number of Link LSAs: 2, checksum sum 75181

*****
Command : show ospfv3-af ipv6 statistics interface all-vrfs
*****
Address-family : IPv6 Unicast
-----

OSPFv3 AF Process ID 1 VRF default, Interface 1/1/1 Statistics (cleared 0h 4m 45s ago)

```

```

=====
==

Tx Hello packets      : 28                Rx Hello packets      : 28
Tx Hello bytes        : 1116              Rx Hello bytes        : 1116
Tx DD packets         : 3                 Rx DD packets         : 2
Tx DD bytes           : 164              Rx DD bytes           : 136
Tx LS request packets : 1                 Rx LS request packets : 1
Tx LS request bytes   : 64                Rx LS request bytes   : 64
Tx LS update packets  : 4                 Rx LS update packets  : 4
Tx LS update bytes    : 368              Rx LS update bytes    : 452
Tx LS ack packets     : 3                 Rx LS ack packets     : 2
Tx LS ack bytes       : 208              Rx LS ack bytes       : 152

Total IPsec packets processed : 10
Total IPsec bytes processed   : 6400
Total Number of State Changes : 3
Number of LSAs                : 2
LSA Checksum Sum              : 60947

Total OSPFv3-AF Packets Discarded: 0
-----

Reason                      Packets Dropped
-----
Invalid Type                 0
Invalid Length               0
Invalid Version              0
Bad or Unknown Source        0
Area Mismatch                0
Self-originated              0
Duplicate Router ID          0
Interface Standby            0
Total Hello Packets Dropped  0
  Hello Interval Mismatch    0
  Dead Interval Mismatch     0
  Options Mismatch           0
  MTU Mismatch               0
  Neighbor Ignored            0
Resource Failures            0
Bad LSA Length               0
Others                       0
IPsec Authentication Errors   0

Total LSAs Ignored : 0
-----
Bad Type           : 0
Bad Length         : 0
Invalid Data       : 0
Invalid Checksum   : 0

OSPFv3 AF Process ID 2 VRF red, Interface 1/1/2 Statistics (cleared 0h 4m 45s ago)
=====

Tx Hello packets      : 28                Rx Hello packets      : 28
Tx Hello bytes        : 1116              Rx Hello bytes        : 1116
Tx DD packets         : 3                 Rx DD packets         : 2
Tx DD bytes           : 144              Rx DD bytes           : 136
Tx LS request packets : 1                 Rx LS request packets : 1
Tx LS request bytes   : 64                Rx LS request bytes   : 52
Tx LS update packets  : 4                 Rx LS update packets  : 4

```

Tx LS update bytes	: 332	Rx LS update bytes	: 452
Tx LS ack packets	: 3	Rx LS ack packets	: 2
Tx LS ack bytes	: 208	Rx LS ack bytes	: 132

Total IPsec packets processed : 10
 Total IPsec bytes processed : 6400
 Total Number of State Changes : 3
 Number of LSAs : 2
 LSA Checksum Sum : 75181

Total OSPFv3-AF Packets Discarded: 0

Reason	Packets Dropped
Invalid Type	0
Invalid Length	0
Invalid Version	0
Bad or Unknown Source	0
Area Mismatch	0
Self-originated	0
Duplicate Router ID	0
Interface Standby	0
Total Hello Packets Dropped	0
Hello Interval Mismatch	0
Dead Interval Mismatch	0
Options Mismatch	0
MTU Mismatch	0
Neighbor Ignored	0
Resource Failures	0
Bad LSA Length	0
Others	0
IPsec Authentication Errors	0

Total LSAs Ignored : 0

Bad Type	: 0
Bad Length	: 0
Invalid Data	: 0
Invalid Checksum	: 0

Command : show ospfv3-af ipv6 virtual-links all-vrfs

Address-family : IPv6 Unicast

Virtual link to router 40.40.40.40 is up

Process ID 21 VRF default, Transit area 0.0.0.1
 Transit delay 1 sec
 Timer Intervals: hello 10, dead 40, retransmit 5
 No authentication
 Number of Link LSAs: 0, checksum sum 0
 4 state changes

[End] Feature ospfv3-af

```
=====
Show Tech commands executed successfully
=====
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

summary-address

```
summary-address <PREFIX/LENGHT> [no-advertise | tag <TAG-VALUE>]
no summary-address <PREFIX/LENGHT> [no-advertise | tag <TAG-VALUE>]
```

Description

Summarizes the external routes with the matching address and mask. When advertising this route, its metric is set to the lowest cost path from among the routes that were summarized.

The **no** form of this command disables route summarization.



This command only works for an ASBR (Autonomous System Boundary Router).

Parameter	Description
<PREFIX/LENGHT>	Specifies the IP prefix/mask for advertising the aggregate route.
no-advertise	Do not advertise the aggregate route. Suppress routes that match the specified prefix/mask pair.
tag <TAG-VALUE>	Specify the tag for the aggregate route. The summary prefix will be advertised along with the tag value in External LSAs. Range: 0 to 4294967295

Examples

Setting OSPFv3 AF route summarization for IPv4:


```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv4-uc)# summary-address 10.1.0.0/16
switch(config-ospfv3-ipv4-uc)# summary-address 10.1.0.0/16 no-advertise
switch(config-ospfv3-ipv4-uc)# summary-address 10.1.0.0/16 tag 10
```

Disabling route summarization for IPv4:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-ipv4-uc)# no summary-address 10.1.0.0/16
switch(config-ospfv3-ipv4-uc)# no summary-address 10.1.0.0/16 no-advertise
switch(config-ospfv3-ipv4-uc)# no summary-address 10.1.0.0/16 tag 10
```

Setting OSPFv3 AF route summarization for IPv6:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-ipv6-uc)# summary-address fd00::1/64
switch(config-ospfv3-ipv6-uc)# summary-address fd00::1/64 no-advertise
switch(config-ospfv3-ipv6-uc)# summary-address fd00::1/64 tag 10
```

Disabling route summarization for IPv6:

```
switch(config)# router ospfv3 1
switch(config-ospfv3-ipv6-uc)# no summary-address fd00::1/64
switch(config-ospfv3-ipv6-uc)# no summary-address fd00::1/64 no-advertise
switch(config-ospfv3-ipv6-uc)# no summary-address fd00::1/64 tag 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-ospfv3-ipv4-uc<PROCESS-ID>	Administrators or local user group members with execution rights for this command.
9300S	config-ospfv3-ipv6-uc<PROCESS-ID>	

timers lsa-arrival

```
timers lsa-arrival <DELAY>
no timers lsa-arrival
```

Description

Configures the minimum delay between receiving the same LSA from a peer. The same LSA is an LSA that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives before the delay expires, the LSA is dropped. Generally, the LSA arrival timer should be set

to a value less than or equal to the start-time value for the command **timers throttle lsa** on the neighbor.

The **no** form of this command sets the LSA timers to default values.



Configuration is supported both globally and in the address-family for ipv4-unicast and ipv6-unicast. If disable is configured for the address-family, it will override the global configuration.

Parameter	Description
<code><DELAY></code>	Specifies the delay in milliseconds. Range: 0 to 600000. Default: 1000.

Examples

Setting the LSA arrival timer:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# timers lsa-arrival 10
```

Setting the LSA arrival timer to default:

```
switch(config)# router ospfv3-af 1  
switch(config-ospfv3-af-1)# no timers lsa-arrival
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-af- <code><PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

timers throttle lsa

```
timers throttle lsa start-time <START-TIME> hold-time <HOLD-TIME> max-wait-time <WAIT-TIME>  
no timers throttle lsa
```

Description

Configures the timers for LSA generation.

The **no** form of this command sets the LSA timers to default values.



Configuration is supported both globally and in the address-family for ipv4-unicast and ipv6-unicast. If timers are configured for the address-family, they will override the global configuration.

Parameter	Description
<code>start-time <START-TIME></code>	Specifies the initial wait time in milliseconds after which LSAs are generated. When set to 0, the LSAs are generated without any delay. Range: 0 to 600000. Default: 5000.
<code>hold-time <HOLD-TIME></code>	Specifies the amount of time, in milliseconds, between regeneration of an LSA. The hold time doubles each time the same LSA must be regenerated, until max-wait-time is reached. When set to 0, LSA regeneration time is not increased. Range: 0 to 600000. Default: 0.
<code>max-wait-time <WAIT-TIME></code>	Specifies the maximum wait time, in milliseconds, for regeneration of the same LSA. When set to 0, LSA regeneration time is not increased. Range: 0 to 600000. Default: 0.

Examples

Setting the LSA timers:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# timers throttle lsa start-time 100 hold-time 1000 max-wait-time 10000
```

Setting LSA timers to default values:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# no timers throttle lsa
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config-ospfv3-af-<PROCESS-ID></code>	Administrators or local user group members with execution rights for this command.

timers throttle spf

```
timers throttle spf start-time <milliseconds> hold-time <milliseconds>
max-wait-time <milliseconds>
no timers throttle spf
```

Description

Configures timers for SPF calculation. There are three timers:

- **start-time:** Is the initial delay before an SPF calculation is started. Default is 200 milliseconds.
- **hold-time:** Is the progressive backoff time to wait before next scheduled SPF calculation. Default is 1000 milliseconds. If a route change event occurs during this period, the value doubles until it reaches the *max-wait-time*.
- **max-wait-time:** Is the maximum time to wait before the next scheduled SPF calculation. Default is 5000 milliseconds. This is used to limit the SPF hold timer and also defines the time to be considered for which the OSPF LSDB has to be stable, after which the SPF throttle mechanism is reset.

The **no** form of this command sets all the configured non-default timers to default value.



The configuration is supported globally as well as per address-families ipv4-unicast or ipv6-unicast. If address-family specific timers is configured, it takes precedence over global configuration.

Parameter	Description
<START-TIME>	Time in milliseconds to set timer for initial SPF delay. Default: 200. Range: 1-600000 <i>Required</i>
<HOLD-TIME>	Time in milliseconds to set the minimum hold time between two consecutive SPF calculations. Default: 1000. Range: 1-600000 <i>Required</i>
<WAIT-TIME>	Time in milliseconds to set the maximum wait time between two consecutive SPF calculations. Default: 5000. Range: 1-600000 <i>Required</i>

Examples

Setting non-default timer values for SPF throttling:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# timers throttle spf start-time 100 hold-time 1000 max-
wait-time 10000
```

Setting default timer values for SPF throttling after configuring non-default values:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# no throttle spf
switch(config-ospfv3-af-1)# no timers throttle spf start-time 100 hold-time 1000
max-wait-time 10000
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-ospfv3-af- <i><PROCESS-ID></i>	Administrators or local user group members with execution rights for this command.

transit-delay

```
transit-delay <seconds>
no transit-delay
```

Description

Sets the time delay in Link state transmission for virtual links.

The **no** form of this command sets the delay in Link state transmission to the default of 1 second for virtual links.

Parameter	Description
<i><seconds></i>	Specifies the time delay for the transit delay, in seconds. Range: 1 to 3600. Default: 1.

Examples

Setting OSPFv3 AF virtual links transit delay:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# transit-delay 30
```

Setting OSPFv3 AF virtual links transit delay to default:

```
switch(config)# router ospfv3-af 1
switch(config-ospfv3-af-1)# address-family ipv6 unicast
switch(config-ospfv3-ipv6-uc)# area 100 virtual-link 100.0.1.1
switch(config-router-vlink6)# no transit-delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-router-vlink	Administrators or local user group members with execution rights for this command.

packet-capture commands

copy packet-capture

`copy packet-capture-pcap <FILE_NAME> <REMOTE_URL>`

Description

This command copies a capture file created using the [packet-capture](#) to a remote URL.

Parameter	Description
<code><FILE_NAME></code>	Specifies the name of the <i>tcpdump</i> capture file to be copied.
<code><REMOTE_URL></code>	Specifies a URL to copy the command output. Valid URL syntaxes: ■ <code>sftp://USER@{IP HOST}[:PORT]/FILE</code> ■ <code>tftp://{IP HOST}[:PORT][;blocksize=VAL]/FILE</code>

Example

```
8400x# copy packet-capture-pcap my_capture_file.pcap
sftp://root@10.0.0.2/file.pcap
root@10.0.0.2's password:
Connected to 10.0.0.2.
sftp> put my_capture_file.pcap file.pcap
Uploading my_capture_file.pcap to /root/file.pcap
my_capture_file.pcap 100% 156 219.8KB/s 00:00
Copied successfully.
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
5420	config	Administrators or local user group members with execution rights for this command.
6200		
6300		
6400		
8100		
8325		
8360		
9300		
10000		

packet-capture delete-pcap

```
packet-capture delete-pcap <FILE_NAME>
```

Description

This command deletes a capture file created with the [packet-capture](#) command.

Parameter	Description
<i><FILE_NAME></i>	Specifies the name of the <i>tcpdump</i> capture file to be deleted.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
5420	config	Administrators or local user group members with execution rights for this command.
6200		
6300		
6400		
8100		
8325		
8360		
9300		
10000		

packet-capture enable

```
packet-capture <SESSION_NAME> [enable]
```

no...

Description

Enables the packet capture session.

The **no** form of this command disables the packet capture for the specified session.

Parameter	Description
<SESSION_NAME>	Specifies the session name.
enable	Enables packet capture for the specified session.



Note: A session name must be specified first before issuing the *enable* command or its *no* form. If the session hasn't been configured as a [packet-capture](#) session prior to running these commands, the error message *Packet Capture session does not exist* is displayed.

Examples

Enable packet capture for *session1*:

```
switch# packet-capture session1 enable
```

Disable packet capture for *session1*:

```
switch# no packet-capture session1 enable
```



Note: If *session1* has been configured as a [packet-capture](#) session but isn't enabled, the error message *Packet Capture session not running* is displayed when issuing the *no* form of the command.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
5420 6200 6300 6400 8100	config	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8325		
8360		
9300		
10000		

packet-capture

```
packet-capture <SESSION_NAME> <PORT-ID> ( mac { <SMAC> <DMAC> <ETHERTYPE> } | ipv4
{<PROTOCOL> <SIP> eq <SPORT> <DIP> eq <DPORT> } | ipv6 {<PROTOCOL> <SIP> eq <SPORT> <DIP>
eq <DPORT> }) file-name <PCAP_NAME> [timeout <TIMEOUT>] [buffer-size <BUFFER_SIZE>] [sw-
filter <SW_FILTERS>] [vlan <VLAN>]
```

Description

Configures a new packet capture session.

Parameter	Description
<SESSION_NAME>	Configures the session name with a maximum of 32 characters.
<PORT-ID>	Configures the port ID. Applies to physical ports only.
<SMAC>	Configures the source MAC address.
<DMAC>	Configures the destination MAC address.
<ETHERTYPE>	Configures either a hexadecimal <i>EtherType</i> value (<H:600–FFFF>) or a supported protocol name (arp, fcoe, fcoe-init, ip, ipv6, ipx-arpa, ipx-non-arpa, is-is, lldp, mpls-multicast, mpls-unicast, q-in-q, rbridge, trill, wake-on-lan).
<PROTOCOL>	Configures either a numeric protocol value (0–255) or a supported protocol name (ah, any, esp, gre, icmp, igmp, ip, ospf, pim, sctp, tcp, udp).
<SIP>	Configures the source IP address.
<DIP>	Configures the destination IP address.
<SPORT>	Configures the source port.
<DPORT>	Configures the destination port.
<TIMEOUT>	Configures the maximum session time for packet capture in seconds. Default: 300.

Parameter	Description
<BUFFER_SIZE>	Configures the buffer size in MB. Range: 1-100. Default: 100.
<PCAP_NAME>	Configures the packet capture file name. Length: 5-128 characters.
<SW_FILTERS>	Configures the software filter with a maximum of 512 characters. Standard <i>tcpdump</i> filters are supported for this parameter.
<VLAN>	Configures the VLAN identifier. Range: 1-4094.

Examples

Packet capture using MAC:

```
switch# packet-capture session1 1/1/1 mac 0050.5696.7cef 0050.5696.7cea 0800
```

Packet capture using IPV4:

```
switch# packet-capture session1 1/1/1 ipv4 tcp any eq any any eq any
```

Packet capture using IPV6:

```
switch# packet-capture session1 1/1/1 ipv6 any 2001:db8:abcd:12::2/ffff:ffff::0000
eq any any eq any
```

General Limitations

- Only 3 *pcap* files are allowed at one time. Creating a fourth *pcap* file will replace the oldest one.
- Packet capture is only supported on physical ports.
- Only one `packet-capture` session can be active a time.
- A `packet-capture` session cannot be active at the same time as a mirror session with destination CPU.
- Packets captured by `packet-capture` sessions will not include the Ethernet *frame check* sequence in the resulting capture.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
5420	config	Administrators or local user group members with execution rights for this command.
6200		
6300		
6400		
8100		
8325		
8360		
9300		
10000		

packet-capture commands

show packet-capture pcaps

```
show packet-capture pcaps
```

Description

This command shows capture files created with the [packet-capture](#) command.

Parameter	Description
pcaps	Lists the saved <i>tcpdump</i> capture files.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
5420	config	Administrators or local user group members with execution rights for this command.
6200		
6300		
6400		
8100		
8325		
8360		
9300		
10000		

show packet-capture session

show packet-capture [<SESSION_NAME>]

Description

Displays information about packet capture sessions configured on the switch. If a *SESSION_NAME* is specified, it shows details for that session only.

Parameter	Description
<SESSION_NAME>	Specifies the name of the packet capture session.

Examples

Packet capture using MAC:

```
switch# show packet-capture
Name                : orange0
Admin State         : Disabled
Operation Status    : Inactive
Reason code         : max-timeout-reached
Port                : 1/1/1
Hardware filter     : ipv4
  Ethertype         : -
  Source MAC        : -
  Dest MAC          : -
  Source IP         : -
  Destination IP    : -
  Protocol          : -
  Source port min   : 21
  Source port max   : 21
  Dest port min     : 1001
  Dest port max     : 1001
  Vlan              : -
Software Filter     : -
Buffer size (in MB) : 100
Timeout (in second) : 300
Pcap file name      : session1.pcap
Capture direction   : Ingress and egress
```



On 5420, 6200, 6300, 6400, 8100 and 8360 Switch Series, both *ingress* and *egress* are supported capture directions.

On 8325, 9300 and 10000 Switch Series, only *ingress* is a supported capture direction.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
5420	config	Administrators or local user group members with execution rights for this command.
6200		
6300		
6400		
8100		
8325		
8360		
9300		
10000		

apply policy

```
apply policy <POLICY-NAME> routed-in  
no apply policy <POLICY-NAME> routed-in
```

Description

Applies a classifier policy containing a PBR action to an interface. A policy with PBR actions is only applicable to L3/routing interfaces.

The **no** form of this command removes a classifier policy containing a PBR action from an interface.
config-if

Parameter	Description
<POLICY-NAME>	Specifies name of the policy.

Restrictions

- Only Layer 3 interfaces are valid for PBR policy application, and only in the routed inbound direction.
- If a policy with an 'interface tunnel' PBR action is applied on a Layer 3 interface in VRF 'A', and that interface tunnel is a member of VRF 'B', the interface tunnel is considered down/unavailable in this policy application in VRF 'A'.

Usage

To use route-only ports (ROPs) as Layer 3 interfaces, an internal VLAN range must be configured first. A policy with PBR actions can be applied to ROPs.

Example

On the HPE Aruba Networking 6400 Switch Series, interface identification differs.

Applying a policy to an interface:

```
switch(config)# interface 1/1/10.10  
switch(config-if)# routing  
switch(config-if)# apply policy pbr_policy routed-in  
switch(config-if)# exit
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

pbr-action-list

pbr-action-list <ACTION-LIST-NAME>

```
[<SEQUENCE-NUMBER>]
{nexthop | default-nexthop} <NEXT-HOP-IP-ADDR>
interface {null | <TUNNEL-NAME>}

no [<SEQUENCE-NUMBER>]
{nexthop | default-nexthop} <IP-ADDR>
interface {null | <TUNNEL-NAME>}
```

no pbr-action-list <ACTION-LIST-NAME>

Description

Creates a PBR action list or modifies its entries.

The **no** form of this command can be used to delete an action list or an individual action list entry.

Parameter	Description
<ACTION-LIST-NAME>	Specifies the action list name. An action list name can be 1 to 64 alphanumeric characters.
<SEQUENCE-NUMBER>	Specifies list entry sequence number. Range: 1-4294967295 {nexthop default-nexthop} Selects a regular next-hop (nexthop) or a default next-hop (default-nexthop). These parameters specify the address of a next-hop router to forward traffic matched by a class under different conditions.
nexthop	Sets the next hop for routing the packet.
default-nexthop	Sets the next hop for routing the packet when there is no explicit route for its destination.
<NEXTHOP-IP-ADDR>	Specifies IPv4 or IPv6 address of the next-hop router.
interface {null <TUNNEL-NAME>}	Selects the type of keyword interface: null or the tunnel interface name.
interface null	Selects keyword interface: null .
null	Specifies to drop matching traffic.

Parameter	Description
<code><TUNNEL-NAME></code>	Specifies an IP tunnel interface name through which to forward the matching traffic.

Restrictions

The reachability of the next-hop routers/tunnel interfaces in the list is not guaranteed. Such reachability can change at any time due to the dynamic nature of the network environment.

Usage

Each action list may contain up to eight entries of four different entry types:

- `interface null`
- `interface tunnel`
- `nexthop`
- `default-nexthop`

List entries have a unique sequence number which, if not user specified, are automatically assigned beginning at 10 and continuing at intervals of 10 for each subsequent new list entry, for example 20, 30, and 40. Sequence numbers of any value can be specified manually, a different interval may be set, and new entries can be added to (or removed from) any location in the list at any time.

Specifying an existing sequence number causes the existing list entry to be replaced by the new details. The list entry with the lowest sequence number has the highest priority entry in the list. The sequence numbers may be renumbered with the [pbr-action-list resequence](#) command.

Only one next-hop router or interface from the list is used per packet matched. This router or interface is defined as the highest priority list entry that is reachable or available at the time of the traffic match. If the highest priority list entry next-hop router or tunnel interface is reachable - that list entry is chosen, the search is stopped, and the traffic is forwarded to the next-hop router or interface for the entry. If the highest priority list entry next-hop router or tunnel interface is not reachable, the next highest priority list entry reachability is determined and used if reachable, otherwise the process continues down the list. If none of the routers in the list are reachable, the packet may be dropped (through the null interface entry if configured) or forwarded according to a system route table entry.



An action list that contains a next-hop of one IP version cannot also contain an entry of another IP version. For example, an action list must contain only IPv4 or IPv6 next-hop addresses or tunnel interfaces.

Examples

The list name is included in the context prompt for easy current-list identification. Any list name over 10 characters will be truncated at 10 characters and terminated with the tilde character (~) to indicate a reduced list name display. This reduction affects the prompt display of the list name only:

```
switch(config)# pbr-action-list eighteenchars
switch(config-pbr-action-list-eightench~)#
```

The following example creates an action list with two IPv4 next-hops, a default IPv4 next-hop, and a null interface. The example uses default sequence numbering for its list entries.


```

switch(config)# pbr-action-list test1
switch(config-pbr-action-list-test1)# nexthop 1.1.1.1
switch(config-pbr-action-list-test1)# nexthop 2.2.2.2
switch(config-pbr-action-list-test1)# default-nexthop 9.9.9.9
switch(config-pbr-action-list-test1)# interface null
switch(config-pbr-action-list-test1)# end

switch(config)# show pbr-action-list test1

```

Sequence	Name Type	Address/Interface

	test1	
10	nexthop	1.1.1.1
20	nexthop	2.2.2.2
30	default-nexthop	9.9.9.9
40	interface	null

The following example creates an action list with an IPv4 next-hop and a tunnel interface with manual sequence numbers for its entries.

```

switch(config)# pbr-action-list test2
switch(config-pbr-action-list-test2)# 6 ip default-nexthop 4.4.4.4
switch(config-pbr-action-list-test2)# 1 interface tunnel10
switch(config-pbr-action-list-test2)# end

switch(config)# show pbr-action-list test2

```

Sequence	Name Type	Address/Interface

	test2	
1	interface	tunnel10
6	default-nexthop	4.4.4.4

The following example creates an action list with two IPv4 tunnel interfaces, with default sequence numbering.

```

switch(config)# pbr-action-list test3
switch(config-pbr-action-list-test3)# interface tunnel10
switch(config-pbr-action-list-test3)# interface tunnel15
switch(config-pbr-action-list-test3)# end

switch(config)# show pbr-action-list test3

```

Sequence	Name Type	Address/Interface

	test3	
10	interface	tunnel10
20	interface	tunnel15

The following example creates an action list with two IPv6 next-hops and the null interface, with manual sequence numbers.

```
switch(config)# pbr-action-list test4
switch(config-pbr-action-list-test4)# 5 nexthop 2000:abcd::cccc:dddd
switch(config-pbr-action-list-test4)# 6 nexthop 1000:abcd::1234:5678
switch(config-pbr-action-list-test4)# 7 interface null
switch(config-pbr-action-list-test4)# end
```

```
switch(config)# show pbr-action-list test4
```

Sequence	Name Type	Address/Interface
	test4	
5	nexthop	2000:abcd::cccc:dddd
6	nexthop	1000:abcd::1234:5678
7	interface	null



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config The pbr-action-list <ACTION-LIST-NAME> command takes you into the config-pbr- action-list- <ACTION-LIST-NAME> context where you modify entries for a PBR action list.	Administrators or local user group members with execution rights for this command.

pbr-action-list copy

```
pbr-action-list <ACTION-LIST-NAME> copy <DESTINATION-ACTION-LIST-NAME>
```

Description

Copies an existing PBR action list.

Parameter	Description
<ACTION-LIST-NAME>	Specifies the action list name to be copied.
<DESTINATION-ACTION-LIST-NAME>	Specifies the name of the copied action list. A destination action list name can be 1 to 64 alphanumeric characters.

Examples

The following example copies test4 action list to test 5.

```
switch(config)# show pbr-action-list test4
```

Sequence	Name Type	Address/Interface

	test4	
5	nexthop	2000:abcd::cccc:dddd
6	nexthop	1000:abcd::1234:5678
7	interface	null

```
switch(config)# pbr-action-list test4 copy test5
switch(config-pbr-action-list-test4)# show pbr-action-list test5
```

Sequence	Name Type	Address/Interface

	test4	
1	nexthop	2000.abcd::cccc.dddd
11	nexthop	1000.abcd::1234.5678
21	interface	null



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

pbr-action-list resequence

`pbr-action-list <ACTION-LIST-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>`

Description

Renumbers the entries in an action list. The list entry with the lowest sequence number has the highest priority entry in the list.

Parameter	Description
<code><ACTION-LIST-NAME></code>	Specifies the action list name to have its entries resequenced.

Parameter	Description
<STARTING-SEQUENCE-NUMBER>	Specifies the starting sequence number. Range: 1-4294967295
<INCREMENT>	Specifies the increment of the resequencing. Range: 1-4294967295

Examples

The following command shows how a PBR action list is resequenced. In the following example, an action list named **test4** is resequenced so that instead of its entries starting at 5 and being numbered sequentially, its entries start now at 1 and they are numbered in increments of 10:

```
switch(config)# show pbr-action-list test4
```

Sequence	Name Type	Address/Interface

	test4	
5	nexthop	2000.abcd::cccc.ddd
6	nexthop	1000.abcd::1234.5678
7	interface	null

```
switch(config)# pbr-action-list test4 resequence 1 10
```

Sequence	Name Type	Address/Interface

	test4	
1	nexthop	2000.abcd::cccc.ddd
11	nexthop	1000.abcd::1234.5678
21	interface	null



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

pbr-action-list reset

```
pbr-action-list <ACTION-LIST-NAME> reset
```

Description

Resets a specified PBR action list to its last successful configuration.

Parameter	Description
<code><ACTION-LIST-NAME></code>	Specifies the action list name to be reset.

Examples

```
switch(config)# pbr-action-list test reset
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

policy

`policy <POLICY-NAME>`

```
[<SEQUENCE-NUMBER>]
  class {ip|ipv6|mac} <CLASS-NAME>
  action {<REMARK-ACTIONS> | <POLICE-ACTIONS> | <OTHER-ACTIONS>}
  [{<REMARK-ACTIONS> | <POLICE-ACTIONS> | <OTHER-ACTIONS>}]
```

```
[<SEQUENCE-NUMBER>]
  comment ...
```

`no policy <POLICY-NAME>`

Description

Creates, modifies, or deletes a classifier policy. A policy contains one or more policy entries ordered and prioritized by sequence numbers. Each entry has an IPv4/IPv6/MAC class and one or more policy actions associated with it. An applied policy processes a packet sequentially against policy entries in the list until the last entry in the list has been evaluated or the packet matches an entry. If a match occurs the related entry, actions are taken.

The **no** form of this command is used to delete a policy or an individual policy entry.

Parameter	Description
<code><POLICY-NAME></code>	Specifies the name of the policy.

Parameter	Description
<code><SEQUENCE-NUMBER></code>	Specifies a sequence number for the policy entry. Optional. Range: 1 to 4294967295.
<code>comment</code>	Stores the remaining entered text as a policy entry comment.
<code>class {ip ipv6 mac} <CLASS-NAME></code>	Specifies a type of class, ip for IPv4, ipv6 for IPv6 and mac for a MAC policy. And specifies a class name.
<code><REMARK-ACTIONS></code>	Remark actions can be any of the following options: {pbr <ACTION-LIST> pcsp <PRIORITY> ip-precedence <IP-PRECEDENCE-VALUE> dscp <DSCP-VALUE> local-priority <LOCAL-PRIORITY-VALUE>} where: pbr <ACTION-LIST> Specifies the PBR action list to be used. pcsp <PCP-VALUE> Specifies Priority Code Point (PCP) value. Range: 0 to 7. ip-precedence <IP-PRECEDENCE-VALUE> Specifies the numeric IP precedence value. Range: 0 to 7. dscp <DSCP-VALUE> Specifies a Differentiated Services Code Point (DSCP) value. Enter either a numeric value (0 to 63) or a keyword as follows: AF11 - DSCP 10 (Assured Forwarding Class 1, low drop probability) AF12 - DSCP 12 (Assured Forwarding Class 1, medium drop probability) AF13 - DSCP 14 (Assured Forwarding Class 1, high drop probability) AF21 - DSCP 18 (Assured Forwarding Class 2, low drop probability) AF22 - DSCP 20 (Assured Forwarding Class 2, medium drop probability) AF23 - DSCP 22 (Assured Forwarding Class 2, high drop probability) AF31 - DSCP 26 (Assured Forwarding Class 3, low drop probability) AF32 - DSCP 28 (Assured Forwarding Class 3, medium drop probability) AF33 - DSCP 30 (Assured Forwarding Class 3, high drop probability) AF41 - DSCP 34 (Assured Forwarding Class 4, low drop probability) AF42 - DSCP 36 (Assured Forwarding Class 4, medium drop probability) AF43 - DSCP 38 (Assured Forwarding Class 4, high drop probability) CS0 - DSCP 0 (Class Selector 0: Default) CS1 - DSCP 8 (Class Selector 1: Scavenger) CS2 - DSCP 16 (Class Selector 2: OAM) CS3 - DSCP 24 (Class Selector 3: Signaling) CS4 - DSCP 32 (Class Selector 4: Real time)

Parameter	Description
	CS5 - DSCP 40 (Class Selector 5: Broadcast video) CS6 - DSCP 48 (Class Selector 6: Network control) CS7 - DSCP 56 (Class Selector 7) EF - DSCP 46 (Expedited Forwarding) <code>local-priority <LOCAL-PRIORITY-VALUE></code> Specifies a local priority value. Range: 0 to 7.
<code><POLICE-ACTIONS></code>	Police actions can be the following {cir <RATE-BPS> cbs <BYTES> exceed} where: <code>cir <RATE-BPS></code> Specifies a Committed Information Rate value in Kilobits per second. Range: 1 to 4294967295. <code>cbs <BYTES></code> Specifies a Committed Burst Size value in bytes. Range: 1 to 4294967295. <code>exceed</code> Specifies action to take on packets that exceed the rate limit.
<code><OTHER-ACTIONS></code>	Other actions can be the following: <code>drop</code> Specifies drop traffic.

Restrictions

MAC classes are not applicable to policies containing PBR actions. Applying such policies to an interface are blocked.

Usage

- For Policy Based Routing, the policy action keyword is **pbr** which itself takes the name of a PBR action list as a parameter.
- A policy entry that contains a PBR action can contain other action types as well.
- An applied policy processes a packet sequentially against policy entries in the list until the last policy entry in the list has been evaluated or the packet matches an entry.
- Entering an existing **<POLICY-NAME>** value will cause the existing policy to be modified, with any new **<SEQUENCE-NUMBER>** value creating an additional policy entry, and any existing **<SEQUENCE-NUMBER>** value replacing the existing policy entry with the same sequence number.
- If no sequence number is specified, a new policy entry is appended to the end of the entry list with a sequence number equal to the highest policy entry currently in the list plus 10.

Examples

Create a policy with two PBR actions:

```
switch(config)# policy pbr_policy
switch (config-policy)# 10 class ip v4_class action pbr action_list1
switch (config-policy)# 20 class ipv6 v6_class action pbr action_list2
switch (config-policy)# exit
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config The <code>policy</code> command takes you into the <code>config-policy</code> context where you enter the policy entries.	Administrators or local user group members with execution rights for this command.

show pbr

```
show pbr {interface <INTERFACE-NAME>|vrf <VRF-NAME>|summary}
```

Description

Shows a detailed view of Policy Based Routing (PBR) in the system.

Parameter	Description
<VRF-NAME>	Specifies name of a VRF.
<INTERFACE-NAME>	Specifies an interface. Format: member/slot/port .

Usage

Show commands can only reference the default VRF.

Examples

Showing PBR summary information when there is no active next-hop in the system:

```
switch# show pbr summary
VRF      Port    Policy    PBR      Seq  Type      Nexthop
-----
No active PBR nexthop found
-----
```

Showing PBR summary information when there are active next-hops in the system:

```
switch# show pbr summary
VRF      Port    Policy    PBR      Seq  Type      Nexthop
-----
default  1/1/1  policy_1  pbr_1    10   nexthop   1.1.1.1 (active)
          1/1/2  policy_2  pbr_2    20   nexthop   5.5.5.5 (active)
-----
```


Showing PBR summary information when displaying a policy with a **pbr-action-list** applied on a VxLAN L3VNI:

```
switch# configure terminal
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 10000
switch(config-vni-10000)# apply policy p1 routed-in
switch(config-vni-10000)# show pbr summary
VRF
    Port
        Policy
            Class
                PBR
                    Sequence  Type          Nexthop
-----
red
    vni10000
        p1
            c1
                pbr1
                    10  nexthop      11.2.1.4
(active)
-----
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show pbr-action-list

show pbr-action-list [<ACTION-LIST-NAME>] [commands] [configuration] [vsx-peer]

Description

Shows the current PBR action list configuration. Action list entries are displayed in ascending order of their sequence number.

Parameter	Description
<ACTION-LIST-NAME>	Specifies the PBR action list name.

Parameter	Description
commands	Formats output as CLI commands.
configuration	Displays user-specified configuration.
vsx-peer	Displays VSX peer switch information.

Restrictions

If an action list entry is modified to an invalid value (for example through the REST interface), this command will indicate a mismatch for that action entry when run. In this event, use the **pbr-action-list <NAME> reset** command to restore it to the previous valid value.

Usage

- This command does not indicate whether the action list is configured in a policy or applied to an interface. Use the **show pbr** command for PBR status involving action lists.
- A single action list is shown by specifying its name or you can show all action lists by omitting a name argument.
- Using the additional commands keyword, you can change the tabulated output to a configuration style output for single or all list display.

Examples

Create two PBR action lists then run **show pbr-action-list** to display all configured action lists in the default configuration mode:

```
switch(config)# pbr-action-list v4_pbr
switch(config-pbr-action-list-v4_pbr)# 1 nexthop 1.1.1.1
switch(config-pbr-action-list-v4_pbr)# 5 default-nexthop 2.2.2.2
switch(config-pbr-action-list-v4_pbr)# 10 interface null
switch(config-pbr-action-list-v4_pbr)# exit
switch(config)#
switch(config)# pbr-action-list v6_pbr
switch(config-pbr-action-list-v6_pbr)# 20 nexthop 2000:abcd::cccc:dddd
switch(config-pbr-action-list-v6_pbr)# 40 default-nexthop 1000:abcd::1234:5678
switch(config-pbr-action-list-v6_pbr)# 60 interface null
switch(config-pbr-action-list-v6_pbr)# exit
switch#
```

```
switch# show pbr-action-list
      Name
Additional PBR-Action-List Parameters
Sequence   Type                Nexthop
-----
-----
      v4_pbr
1          nexthop          1.1.1.1
5          default-nexthop  2.2.2.2
10         interface        null

      v6_pbr
20         nexthop          2000:abcd::cccc:dddd
40         default-nexthop  1000:abcd::1234:5678
60         interface        null
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config current-context

show running-config current-context

Description

Displays the configuration of the PBR action list in the current configuration context, in commands mode.

Parameter	Description
running-config	Shows configuration currently running on switch.
current-context	Limits display to current config context only, in commands mode.

Usage

Useful for reexamining entries previously entered into the action list after its entries have scrolled off the terminal due to other output or upon reentering the context of an existing action list.

Examples

Creating two PBR action lists and running **show running-configuration curent-context** to display the action list configuration in commands mode:

```
switch(config)# pbr-action-list v4_pbr
switch(config-pbr-action-list-v4_pbr)# 1 nexthop 1.1.1.1
switch(config-pbr-action-list-v4_pbr)# 5 default-nexthop 2.2.2.2
switch(config-pbr-action-list-v4_pbr)# 10 interface null
switch(config-pbr-action-list-v4_pbr)# exit
switch(config)#
switch(config)# pbr-action-list v6_pbr
switch(config-pbr-action-list-v6_pbr)# 20 nexthop 2000:abcd::cccc:dddd
switch(config-pbr-action-list-v6_pbr)# 40 default-nexthop 1000:abcd::1234:5678
switch(config-pbr-action-list-v6_pbr)# 60 interface null
switch(config-pbr-action-list-v6_pbr)#
switch(config-pbr-action-list-v6_pbr)# show running-config current-context
```

```
pbr-action-list v6_pbr
 20 nexthop 2000:abcd::cccc:dddd
 40 default-nexthop 1000:abcd::1234:5678
 60 interface null
```

Switching context back to the first action list and running the same command:

```
switch(config-pbr-action-list-v6_pbr) # pbr-action-list v4_pbr
switch(config-pbr-action-list-v4_pbr) #
switch(config-pbr-action-list-v4_pbr) # show running-config current-context
pbr-action-list v4_pbr
 1 nexthop 1.1.1.1
 5 default-nexthop 2.2.2.2
10 interface null
```

Removing action list entry number 5 and running the command again:

```
switch(config-pbr-action-list-v4_pbr) # no 5
switch(config-pbr-action-list-v4_pbr) # show running-config current-context
pbr-action-list v4_pbr
 1 nexthop 1.1.1.1
10 interface null
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

Backup nexthop group commands

ip nexthop group type backup

```
ip nexthop group <GROUP-NAME> type backup
no ip nexthop group <GROUP-NAME> type backup
```

Description

Creates backup nexthop group with a given name. If the backup nexthop group already exists, this command enters that backup nexthop group's configuration context.

The **no** form of this command deletes the backup nexthop group context and all configuration related to the backup nexthop group.

Parameter	Description
<i><GROUP-NAME></i>	Specifies nexthop group name. Nexthop group name can be a maximum of 64 alphanumeric characters.

Example

Creating a backup nexthop group named **grp1**:

```
switch(config)# ip nexthop group grp1 type backup
switch(config-nexthop-group-grp1)#
```

Deleting a backup nexthop group named **grp1**:

```
switch(config)# ip nexthop group grp1 type backup
switch(config-nexthop-group-grp1)# no ip nexthop group grp1 type backup
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

primary secondary nexthop

```
primary <PRIMARY-NEXTHOP-IP-ADDRESS> <PRIMARY-NEXTHOP-EGRESS-INTERFACE>
secondary <SECONDARY-NEXTHOP-IP-ADDRESS> <SECONDARY-NEXTHOP-EGRESS-INTERFACE>
```

```
no primary <PRIMARY-NEXTHOP-IP-ADDRESS> <PRIMARY-NEXTHOP-EGRESS-INTERFACE>
no secondary <SECONDARY-NEXTHOP-IP-ADDRESS> <SECONDARY-NEXTHOP-EGRESS-INTERFACE>
```

Description

Configures primary and secondary nexthops for the backup nexthop group.

The **no** form of this command removes primary or secondary nexthop for a backup nexthop group.

Parameter	Description
<i><PRIMARY-NEXTHOP-IP-ADDRESS></i>	Specifies primary nexthop's IP address.
<i><PRIMARY-NEXTHOP-EGRESS-INTERFACE></i>	Specifies primary nexthop's egress interface.
<i><SECONDARY-NEXTHOP-IP-ADDRESS></i>	Specifies secondary nexthop's IP address

Parameter	Description
<code><SECONDARY-NEXTHOP-EGRESS-ADDRESS></code>	Specifies secondary nexthop's egress interface.

Usage

- Only one primary and one secondary nexthop per backup nexthop group.
- Configuring more than once will overwrite the previous configuration.
- Primary and secondary nexthop must be configured in the backup nexthop group for the group to be applied.
- Primary and secondary nexthop egress interface must have routing enabled.

Example

Configuring primary and secondary nexthops for a backup nexthop group:

```
switch(config-nexthop-group-grp1)# primary 100.0.0.5 1/1/1
switch(config-nexthop-group-grp1)# secondary 101.0.0.5 1/1/2
```

Configuring primary nexthop for a backup nexthop group with no secondary nexthop configured:

```
switch(config-nexthop-group-grp1)# primary 100.0.0.5 1/1/1
switch(config-nexthop-group-grp1)# secondary 101.0.0.5 1/1/2
switch(config-nexthop-group-grp1)# no secondary 101.0.0.5 1/1/2
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show ip nexthop group name type backup

`show ip nexthop group <GROUP-NAME> type backup`

Description

Shows configuration for backup nexthop group with a given name.

Parameter	Description
<code><GROUP-NAME></code>	Specifies nexthop group name. Nexthop group name can be a maximum of 64 alphanumeric characters.

Example

Showing backup nexthop group configuration:

```
switch# show ip nexthop group grp1 type backup
-----
Nexthop Group: grp1
  Type:                backup
  Primary Nexthop:     100.0.0.5 1/1/1
  Secondary Nexthop:   101.0.0.5 1/1/2
  Config Status:       Valid
  Active Nexthop:      <Primary|Secondary|None>
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip nexthop group type backup

show ip nexthop group type backup

Description

Shows configuration for all backup nexthop groups.

Example

Showing configuration for all backup nexthop groups:

```
switch# show ip nexthop group type backup
-----
Nexthop Group: grp1
  Type:                backup
  Primary Nexthop:     100.0.0.5 1/1/1
  Secondary Nexthop:   101.0.0.5 1/1/2
  Config Status:       Valid
  Active Nexthop:      <Primary|Secondary|None>
-----
Nexthop Group: grp2
  Type:                backup
  Primary Nexthop:     200.0.0.5 1/1/3
  Secondary Nexthop:   201.0.0.5 1/1/4
  Config Status:       Valid
  Active Nexthop:      <Primary|Secondary|None>
-----
Nexthop Group: grp3
  Type:                backup
```

```
Primary Nexthop:      --
Secondary Nexthop:    101.0.0.5 1/1/2
Config Status:        Incomplete
-----
Nexthop Group: grp4
Type:                  backup
Primary Nexthop:      100.0.0.5 1/1/1
Secondary Nexthop:    --
Config Status:        Incomplete
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables PIM globally on the router. PIM is disabled by default.



Using the **disable** command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim
switch(config-pim)# disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables PIM globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim
switch(config-pim)# enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

ip pim-dense

```
ip pim-dense {enable|disable}
no ip pim-dense [enable]
```

Description

Enables or disables PIM-DM in the current interface. PIM-DM is disabled by default on an interface. IP address must be configured on the interface to enable PIM-DM.

Parameter	Description
enable	Specifies PIM-DM on the interface. IP address must be configured on the interface to enable PIM-DM (use the ip address <A.B.C.D/M> command).
disable	Disables PIM-DM on the interface.

Examples

Enabling and disabling PIM-DM in an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-dense enable
switch(config-if-vlan)#
switch(config-if-vlan)# ip pim-dense disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense bfd

```
ip pim-dense bfd [disable]
no ip pim-dense bfd
```

Description

Configures BFD on a per-interface basis for an interface associated with the PIM process.

The **no** form of this command removes the BFD configuration on the interface and sets it to the default configuration.

If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the **ip pim-dense bfd disable** command.

If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the **ip pim-dense bfd** command.

Parameter	Description
disable	Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense bfd
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ip pim-dense bfd
```

Disabling the BFD configuration on the interface and overriding the global setting:

```
switch(config-if-vlan)# ip pim-dense bfd disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip pim-dense graft-retry-interval

```
ip pim-dense graft-retry-interval <INTERVAL-VALUE>
no ip pim-dense graft-retry-interval
```

Description

Configures the interval for which the routing switch waits for the graft acknowledgment from another router before resending the graft request.

The **no** form of this command removes the currently configured value and sets to the default of 3 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the interval the routing switch waits for the graft acknowledgment. Default: 3 seconds. Range: 1-10 seconds.

Usage

Graft packets result when a downstream router transmits a request to join a flow. The upstream router responds with a graft acknowledgment packet. If the graft acknowledgment is not received within the time period of the graft-retry-interval, it resends the graft packet.

Example

Configuring and removing dense graft retry interval on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense graft-retry-interval 5
switch(config-if-vlan)# no ip pim-dense graft-retry-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense hello-delay

```
ip pim-dense hello-delay <DELAY-VALUE>
no ip pim-dense hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The **no** form of this command removes currently configured value and sets to the default of 5 seconds.

Parameter	Description
<DELAY-VALUE>	Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Default: 5 seconds. Range: 0-5 seconds.

Usage

In cases where a new interface activates connections with multiple routers, if all the connected routers send hello packets at the same time, the receiving router could become momentarily overloaded. This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense hello-delay 4
switch(config-if-vlan)# no ip pim-dense hello-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense hello-interval

```
ip pim-dense hello-interval <INTERVAL-VALUE>
no ip pim-dense hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface. The **no** form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameter	Description
<INTERVAL-VALUE>	Required: Specifies the frequency at which PIM Hello messages are transmitted on this interface. Default: 30 seconds. Range: 5-300 seconds.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing dense hello-interval:

```
switch(config)# interface 1/1/4
switch(config-if)# ip pim-dense hello-interval 60
switch(config-if)# no ip pim-dense hello-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense ip-addr

```
ip pim-dense ip-addr {<IP-ADDR-VALUE> | any}  
no ip pim-dense ip-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM packets sent from the interface or to use the specific IP address.

The **no** form of this command removes the currently configured value and sets to the default of **any**.

Parameter	Description
<IP-ADDR-VALUE>	Specifies an IP address as the source IP for the interface.
any	Specifies dynamically determining the source IP from the current IP address of the interface.

Examples

Configuring and removing source IP address:

```
switch(config)# interface vlan40  
switch(config-if-vlan)# ip pim-dense ip-addr 40.0.0.4  
switch(config-if-vlan)# no ip pim-dense ip-addr
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	
	config-lag-if	

ip pim-dense lan-prune-delay

```
ip pim-dense lan-prune-delay
no ip pim-dense lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default status is enabled. The **no** form of this command disables the LAN prune delay option.

Usage

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense lan-prune-delay
switch(config-if-vlan)# no ip pim-dense lan-prune-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-if-vlan	
	config-lag-if	

ip pim-dense max-graft-retries

```
ip pim-dense max-graft-retries <ATTEMPT-VALUE>
```



```
no ip pim-dense max-graft-retries
```

Description

Configures the number of attempts the routing switch will retry sending the same graft packet to join a flow.

The **no** form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameter	Description
<code><INTERVAL-VALUE></code>	Specifies the number of retries for the routing switch to resend the graft packet. Default: 3 attempts. Range: 1-10 attempts.

Usage

If a graft acknowledgment response is not received after the specified number of retries, the routing switch ceases trying to join the flow. In this case the flow is removed until either a state-refresh from upstream re-initiates the flow or an upstream router floods the flow. Increasing this value helps to improve multicast reliability.

Example

Configuring and removing dense graft retry interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense max-graft-retries 6
switch(config-if-vlan)# no ip pim-dense max-graft-retries
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense override-interval

```
ip pim-dense override-interval <INTERVAL-VALUE>
no ip pim-dense override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The **no** form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameter	Description
<code><INTERVAL-VALUE></code>	Specifies the override interval of a LAN Prune Delay option in ms. Default: 2500 ms. Range: 500-6000.

Usage

Each router on the LAN expresses its view of the amount of randomization necessary in the Override Interval field of the LAN Prune Delay option. When all routers on a LAN use the LAN Prune Delay Option, all routers on the LAN MUST set their Override_Interval to the largest Override value on the LAN.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense override-interval 4000
switch(config-if-vlan)# no ip pim-dense override-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense propagation-delay

```
ip pim-dense propagation-delay <DELAY-VALUE>
no ip pim-dense propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The **no** form of this command removes currently configured value and sets to the default of 500 ms.

Parameter	Description
<code><DELAY-VALUE></code>	Specifies the propagation delay value in ms. Default: 500 ms. Range: 250-2000 ms.

Usage

The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the link. When all routers on a link use the LAN Prune Delay Option, all routers on the LAN MUST set Propagation Delay to the largest LAN Delay on the LAN.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense propagation-delay 400
switch(config-if-vlan)# no ip pim-dense propagation-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-dense ttl-threshold

```
ip pim-dense ttl-threshold <THRESHOLD-VALUE>
no ip pim-dense ttl-threshold
```

Description

Configures the multicast datagram time-to-live (router hop-count) threshold for the interface. A state-refresh packet with a TTL less than this threshold will not be forwarded out the interface.

The **no** form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameter	Description
<code><THRESHOLD-VALUE></code>	Specifies the time to live threshold. Default: 3 attempts. Range: 0-255.

Usage

The interface connected to the multicast source does not receive state refresh packets and thus is not state-refresh capable. Downstream VLANs in the switches are state-refresh capable. This parameter provides a method for containing multicast traffic within a network, or even within specific areas of a network. Initially, the multicast traffic source sets a TTL value in the packets it transmits. Each time one of these packets passes through a multicast routing device, the TTL setting decrements by 1. If the packet arrives with a TTL lower than the ttl-threshold, the routing switch does not forward the packet. The following aspects of the TTL setting of incoming multicast packets must be considered, before changing this parameter on a routing switch:

- A value that is too high will allow multicast traffic to go beyond the internal network.
- A value that is too low may prevent some intended hosts from receiving the desired multicast traffic.
- A value of 0 will forward multicast traffic regardless of the packet TTL setting.

Example

Configuring and removing the time-to-live threshold:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense ttl-threshold 8
switch(config-if-vlan)# no ip pim-dense ttl-threshold
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

router pim

```
router pim [vrf <VRF-NAME>]
  accept-register access-list <ACL-RULE>
  accept-rp <IP-ADDR> access-list <ACL-RULE>
  active-active
  bfd all-interfaces
```

```

bsr-candidate {bsm-interval <INTERVAL-VALUE> | {hash-mask-length <LENGTH-VALUE> |
priority <PRIORITY-VALUE> | source-ip-interface <INTERFACE-NAME>}
enable|disable
join-prune-interval <INTERVAL-VALUE>
multicast-route-limit <limit>
no ...
register-rate-limit <limit>
rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
rp-candidate {group-prefix <GRP-ADDR/GRP-MASK> |hold-time <TIME-VALUE> | priority
<PRIORITY-VALUE> | source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-
MASK>]}
rpf-override <SRC-ADDR/SRC-MASK><RPF-ADDR|INTERFACE-NAME>

```

Description

Changes the current context to the PIM configuration context and enables PIM globally on the router. If no VRF is specified, the default VRF is assumed.

The **no** form of this command removes the PIM configuration from the specified context or the default VRF.

Parameter	Description
vrf <VRF-NAME>	Specifies the name of a VRF.
accept-register access-list <ACL-RULE>	Specify an ACL rule name to configures ACL on RP to filter PIM Register packets from unauthorized sources. The ACL specified will contain the (S,G) traffic in register packets to permitted or denied.
accept-rp <IP-ADDR> access-list <ACL-RULE>	Specify the IPv4 address of the static RP and ACL rule name to enable the PIM router to filter PIM join/prune messages destined for a specific RP and specific groups. The ACL specifies the group addresses which are allowed or denied. Up to 8 RP addresses and group ACL can be associated with the PIM router. PIM will store the accepted RP address and the associated group ACL. When a join or prune message is received, a RP look up is made for the packet. If the RP is in the configured list and if the group in the join/prune packet is allowed in the ACL, the packet is allowed. Otherwise the packet is dropped. To allow join/prune message from any groups, group address in the ACL can be wild-carded. In this case, only RP address check is performed. This parameter impacts only (*,G) join/prune messages. If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL. Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements. When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received. NOTE: If there is an active flow which is in the SPT,

Parameter	Description
	the traffic flow through the SPT will continue. Only (*,G) join/prune messages are dropped. (S,G) join/prune messages will not be impacted.
active-active	Enables the PIM active-active mechanism per VRF on VSX. The default is disabled. PIM active-active keeps the multicast forwarding state synchronized on both VSX peer devices. Synchronization is achieved by electing the VSX peer that has the highest IP address as a designated router (DR) and the other as Proxy-DR. If you want the multicast traffic to flow through VSX primary, assign higher IP addresses to the interfaces in VSX primary. When the VSX peer that is acting as the DR goes down, traffic is recovered faster since the multicast routes are synchronized.
bfd all-interfaces	Enables BFD on all PIM interfaces. BFD can be disabled at individual PIM interface using the ip pim-sparse bfd disable command.
bsr-candidate	Configure settings for a router that operates as the BSR in a domain.
bsm-interval <INTERVAL-VALUE>	Configures the interval in seconds to send periodic RP-Set messages to all PIM-SM interfaces on a router that operates as the BSR in a domain. This setting must be smaller than the rp-candidate hold-time settings (range of 30 to 255; default 150) configured in the RPs operating in the domain. Default: 60 seconds. Range: 5-300.
hash-mask-length <LENGTH-VALUE>	Controls the distribution of multicast groups among the C-RP, in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) when allocating this distribution. A longer hash-mask-length results in fewer multicast groups, for each block of group addresses assigned to the RPs. Multiple blocks of addresses assigned to each C-RP results in wider dispersal of addresses. Includes enhanced load-sharing for the multicast traffic for the different groups that are used in the domain at the same time. Default: 30 bits. Range: 1-32.
priority <PRIORITY-VALUE>	Configures the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the BSR of the domain. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain.

Parameter	Description
	Default: 0. Range: 0-255
<code>source-ip-interface <INTERFACE-NAME></code>	Configures the router to advertise itself as a candidate PIM-SM BSR on the interface specified, and enables BSR candidate operation. The result makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. One BSR candidate interface is allowed per-router. The Interface can be a VLAN interface (such as <code>vlan15</code>) or routed interfaces (such as <code>lag 1</code> or <code>1 / 1 / 19</code>). PIM-SM must be enabled on this interface (use the ip pim-spase enable command).
<code>enable disable</code>	Enables or disables PIM globally on the router.
<code>join-prune-interval <INTERVAL-VALUE></code>	Configures the frequency at which the router will send periodic join or prune-interval messages. Range 5 to 65535 Default: 60.
<code>multicast-route-limit <limit></code>	Configures the limit on the maximum number of multicast route entries that can be programmed. When the limit is configured, multicast route entries created because of IGMP or MLD membership reports, and multicast route entries created because of multicast streams are restricted to the configured limit. Flows exceeding the configured multicast route limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration prevents creation of new multicast routes when limits are reached. At the time of configuration, if the device has more multicast routes than the configured limit, existing multicast routes continue to exist until they are removed. The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage. Range: 1 to 4294967295.
<code>no...</code>	Negates any configured parameter.
<code>register-rate-limit <limit></code>	Configures the limit on the maximum number of register messages sent per second for every unique (S,G) entry. By default, there is no maximum rate set. When the limit is configured, register messages generation is limited to the configured value. Range: 1 to 4294967295.
<code>rp-address</code>	Statically configures the router as the RP for a specified multicast group or range of multicast groups. When a static RP and a C-RP are configured to support the same multicast groups and the multicast group mask for the static RP is equal to or greater than the same mask for the applicable C-

Parameter	Description
	RP, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a backup RP for the configured group. Without override, the C-RP has precedence over a static RP configured for the same multicast group or groups. This must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv4 multicast addresses (224.0.0.0 - 239.255.255.255). PIM-SM supports a maximum of 8 static RPs per VRF.
<code><IP-ADDR></code>	Specifies the address of the static RP in IPv4 format (x.x.x.x).
<code><GRP-ADDR/GRP-MASK></code>	Specifies the multicast group address in IPv4 format (x.x.x.x) and the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code>override</code>	Specifies higher precedence to static RP over Candidate RP.
<code>rp-candidate</code>	Configure Candidate Rendezvous Point (C-RP) settings.
<code>group-prefix <GRP-ADDR/GRP-MASK></code>	Adds multicast group address to the current Candidate Rendezvous Point (C-RP) configuration by specifying the the multicast group address in IPv4 format (x.x.x.x) and the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code>hold-time <TIME-VALUE></code>	Changes the hold-time a C-RP includes in its advertisements to the BSR. Hold-time is included in the advertisements the C-RP periodically sends to the elected BSR for the domain. Also updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming it has become unavailable. Range: 30 to 250. Default: 150.
<code>priority <PRIORITY-VALUE></code>	Changes the current priority setting for a C-RP. Where multiple C-RP configurations are used to support the same multicast groups, the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority. Range: 0 to 255. Default: 192.
<code>source-ip-interface</code>	Enables the Candidate Rendezvous Point (C-RP) operation, and configures the router to advertise itself as a C-RP to the Bootstrap Router (BSR) for the current domain. This step includes the option to allow the C-RP to be a candidate for all possible multicast groups, or for up to four multicast groups, or ranges of groups. If group-prefix is not given, it considers for all multicast group addresses.
<code><INTERFACE-NAME></code>	Specifies the interface to use as a source for the C-

Parameter	Description
	RP router IP address.
<code>group-prefix <GRP-ADDR/GRP-MASK></code>	Specifies the multicast group address in IPv4 format (x.x.x.x) and the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code>rpf-override</code>	The Reverse Path Forward (RPF) override allows overriding the normal RPF lookup mechanism, and indicates to the router that it may accept multicast traffic on an interface other than the one that the RPF lookup mechanism would normally select. This includes accepting traffic from an invalid source IP address for the subnet or VLAN that is directly connected to the router. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.
<code><SRC-ADDR/SRC-MASK></code>	Specifies the multicast source IPv4 address in IPv4 format (x.x.x.x) and the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code><RPF-ADDR INTERFACE-NAME></code>	Specifies the RPF override IP address or interface.

Usage

When a register ACL is associated with a PIM Router, the PIM protocol will store the source and destination address details along with the action (permit or deny). If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Upon receiving the register messages, a look up is made to check if the S and G in the packet is in the permitted list. If there is no match or if there is a deny rule match, a register stop message is immediately sent and the packet is dropped and no further action is taken. Permitted packets will go through the normal flow.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Recommendations for the active-active mechanism:

- Do not configure the DR priority of interfaces when **active-active** is enabled. The DR priority will be set to high on DR and default on Proxy-DR and any user-configured DR priority will be ignored.
- Always configure **keepalive** between VSX peers. If the ISL goes down when **keepalive** is not configured, both VSX peers start acting independently as DRs, resulting in duplicate traffic.
- Do not configure IGMP joins on transit VLANs.
- RP redundancy is not supported on the **active-active** mechanism. If one of the VSX peers is configured as RP and it goes down, the new traffic flows will not be converged until the RP is elected. For a static RP, new flows will never be converged until the VSX peer is back up.

Reverse Path Forward (RPF) override usage details:

- Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the

RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.

- RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified. The RPF-address indicates one of two distinct RPF candidates:
 1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of **<source-addr/src-mask>**.
 2. A local router address on a PIM-enabled interface to which **<source-addr/src-mask>** is directly connected. If configured, the local router will assume the role of DR for this flow and registers the flow with an RP.

Examples

Configuring and enabling default router PIM:

```
switch(config)# router pim
switch(config-pim)#enable
```

Configuring specified router PIM:

```
switch(config)# router pim vrf green
switch(config-pim)#
```

Configuring ACL on RP with an ACL rule named **pim_reg_acl**:

```
switch(config)# access-list ip pim_reg_acl
switch(config-acl-ip)# 10 permit any 20.1.1.1 225.1.1.2
switch(config-acl-ip)# 20 deny any 30.1.1.1 225.1.1.3
switch(config)# router pim
switch(config-pim)# accept-register acces
```

Configuring ACL on a RP with an ACL rule named **pim_rp_grp_acl** to filter join/prune messages:

```
switch(config)# access-list ip pim_rp_grp_acl
switch(config-acl-ip)# 10 permit any any 225.1.1.2/255.255.255.0
switch(config-acl-ip)# 20 permit any any 239.1.1.2/255.255.255.0
switch(config-acl-ip)# router pim
switch(config-pim)# accept-rp 30.1
```

Configuring and removing the BSR-candidate interface:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim)# bsr-candidate source-ip-interface vlan5
switch(config-pim)# no rp-candidate source-ip-interface 1/1/4
```

Configuring and removing the multicast route rate limit:

```
switch(config)# router pim  
switch(config-pim)# mcast-route-limit 1024  
switch(config-pim)# no mcast-route-limit
```

Configuring and removing the register rate limit:

```
switch(config)# router pim  
switch(config-pim)# register-rate-limit 10  
switch(config-pim)# no register-rate-limit
```

Configuring and removing candidate-RP router priority and hold times

```
switch(config)# router pim  
switch(config-pim)# rp-candidate priority 250  
switch(config-pim)# rp-candidate hold-time 200
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show ip mroute

```
show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows mroute information for all VRFs. Optional.
vrf <VRF-NAME>	Shows mroute information for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF. Optional.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP mroute for all VRFs:

```
switch# show ip mroute all-vrfs
VRF : blue
Total number of entries : 1

Group Address      : 239.1.1.1
Source Address     : 40.0.0.5
Incoming interface : vlan3
Downstream Interface
Interface  State
-----  ----
vlan2      forwarding

VRF : green
Total number of entries : 2

Group Address      : 239.1.1.1
Source Address     : 40.0.0.4
Neighbor           : 10.1.1.1
Incoming interface : vlan2
Downstream Interface
Interface  State
-----  ----
vlan5      forwarding

Group Address      : 239.1.1.1
Source Address     : 40.0.0.5
Neighbor           : 10.1.1.2
Incoming interface : vlan1
Downstream Interface
Interface  State
-----  ----
vlan6      forwarding

VRF : default
Total number of entries : 1

Group Address      : 10.1.1.14
Source Address     : 40.0.0.6
Neighbor           : 10.1.1.2
Incoming interface : 1/1/5
Downstream Interface
Interface  State
-----  ----
1/1/3      forwarding
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute group-addr

```
show ip mroute <GROUP-ADDR> [<SOURCE-ADDR>] [all-vrfs | vrf <vrf-name>] [vsx-peer]
```

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<GROUP-ADDR>	Specifies a group address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<SOURCE-ADDR>	Specifies show information for the group from this source in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
all-vrfs	Shows mroute information for the group for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group 239.1.1.1 and VRF green:

```
switch# show ip mroute 239.1.1.1 vrf green

VRF : green

Group Address           : 239.1.1.1
Source Address          : 40.0.0.5
Neighbor                : 10.1.1.2
Incoming interface      : vlan1
Unicast Routing Protocol : connected
Metric                  : 1234
Metric Pref              : 1234
Downstream Interface
Interface   State
-----
```

vlan6 forwarding

Showing information for group 239.1.1.1 from source 40.0.0.5 and all VRFs:

```
switch# show ip mroute 239.1.1.1 40.0.0.5 all-vrfs
```

VRF : blue

```
Group Address      : 239.1.1.1
Source Address     : 40.0.0.5
Incoming interface : vlan3
Unicast Routing Protocol : connected
Metric            : 1234
Metric Pref       : 1234
Downstream Interface
Interface State
-----
vlan2 forwarding
```

VRF : green

```
Group Address      : 239.1.1.1
Source Address     : 40.0.0.5
Neighbor          : 10.1.1.2
Incoming interface : vlan1
Unicast Routing Protocol : connected
Metric            : 1234
Metric Pref       : 1234
Downstream Interface
Interface State
-----
vlan6 forwarding
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute brief

```
show ip mroute brief [al-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>all-vrfs</code>	Shows mroute information for all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IP mroute brief:

```
switch# show ip mroute brief
VRF : default
Total number of entries : 1

Group Address      Source Address      Neighbor      Interface
-----
239.1.1.1          40.0.0.6            10.1.1.2      vlan5
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim

```
show ip pim [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>all-vrfs</code>	Optional. Shows PIM router information on all VRFs.
<code>vrf <VRF-NAME></code>	Optional. Shows PIM router information for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP PIM router:

```
switch# show ip pim

PIM Global Parameters

VRF                : default
PIM Status          : Enabled
Join/Prune Interval (sec) : 60
SPT Threshold       : Enabled
State Refresh Interval (sec) : 60
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface

```
show ip pim interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	(Optional) Shows PIM interface information for all VRFs.
vrf <VRF-NAME>	(Optional) Shows PIM interface information for a particular VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface for the HPE Aruba Networking 5420, 6200, 6300, 6400,8100, 8325, 8360, 9300/9300S, 10000 Switch series:

```
switch# show ip pim interface

PIM Interfaces

VRF: default
Total Number of interfaces: 1

Interface           : vlan10
Neighbor count      : 0
IP Address           : 100.100.1.2/24
Mode                 : bidir
Proxy DF             : false
Hello Interval(sec)  : 30
Hello Delay(sec)     : 5
Override Interval(msec) : 2500
Lan Prune Delay      : Yes
Propagation Delay (msec): 500
Neighbor Timeout     : 0
PIM Interfaces

VRF: default

Interface      IP Address      mode
-----
1/1/1          40.0.0.4/24     sparse
1/1/2          50.0.0.4/24     sparse
```

Showing PIM interface:



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Added support for BIDIR PIM on the 6200, 6300, 6400,8100, 8325, 8360, 9300, 10000

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name

show ip pim interface <INTERFACE-NAME> [vsx-peer]

Description

Shows detailed information about the PIM interface currently configured.

Parameter	Description
<INTERFACE-NAME>	Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface information for interface 1/1/2:

```
switch# show ip pim interface 1/1/2

PIM Interfaces

VRF: default

Interface   : 1/1/2
IP Address  : 50.0.0.4/24
Mode        : dense

Designated Router :
Hello Interval (sec)      : 30
Hello Delay (sec)         : 5
Graft Retry Interval(sec) : 3
Max Graft Retries         : 5
SR TTL Threshold          : 8

Override Interval (msec)  : 2500
Propagation Delay (msec)  : 500
Neighbor Timeout          : 105

Lan Prune Delay           : Yes
DR Priority                 : 1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name counters

show ip pim interface <INTERFACE-NAME> counters [vsx-peer]

Description

Shows the PIM packet counters information for the specified interface.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to show packet counter information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM packet counters:

```
switch# show ip pim interface vlan1 counters
Interface      : vlan1
VRF            : default

              Rx          Tx          Drops
              -----
Hello          21          21          0
BSM            12          10         0
Register       0           0          0
SSM Register   5           0          0
Register Stop  0           0          0
SSM Register Stop 0         5          0
Join/Prune     0           0          0
SSM Join/Prune 2           2          0
C-RP Advertisement 0         0          0
Graft          0           0          0
Graft Ack      0           0          0
Assert         0           0          0
State Refresh  0           0          0
Register Drops(Register ACL hitcount) 0         0          4
Join/Prune Drops(RP ACL hitcount)      0         0          7
Unknown Multicast 0         0          0
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rpf

```
show ip pim rpf [<IP-ADDRESS>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Displays PIM RPF details for the specified source or RP address in the given VRF and shows the nexthop and interface through which the shortest path to the source is available. It also displays if a PIM neighbor is present on the nexthop. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<IP-ADDRESS>	(Optional) Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. Shows PIM RPF details for the given IP address.
all-vrfs	(Optional) Shows PIM interface information for all VRFs.
vrf <VRF-NAME>	(Optional) Shows PIM interface information for a particular VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing PIM RPF information for the default VRF:

```
switch# show ip pim rpf
Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
               O - OSPF, B - BGP, R - RIP
```

```

VRF: default
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask
Origin In Use
-----
-   ---
1.1.1.1         vlan10         10.1.1.1       yes             1.1.1.1/32      O
yes
10.1.1.1        vlan10         no             10.1.1.0/24     C
yes
10.1.1.2        vlan10         no             10.1.1.2/32     C
yes

```

Showing PIM RPF information for the specified IP address:

```

switch# show ip pim rpf 1.1.1.1
Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
O - OSPF, B - BGP, R - RIP

VRF: default
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask    Origin
In Use
-----
-----
1.1.1.1         vlan10         10.1.1.1       yes             1.1.1.1/32        O
yes

```

Showing PIM RPF information for all VRFs:

```

switch# show ip pim rpf all-vrfs
Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
O - OSPF, B - BGP, R - RIP

VRF: default
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask    Origin In
Use
-----
-----
--
1.1.1.1         vlan10         10.1.1.1       yes             1.1.1.1/32        O
yes
10.1.1.1        vlan10         no             10.1.1.0/24     C
yes
10.1.1.2        vlan10         no             10.1.1.2/32     C
yes

VRF: red
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask    Origin In
Use
-----
-----
----
2.2.2.2         vlan20         20.0.0.1       yes             2.2.2.2/32        SU
yes
20.0.0.1        vlan20         no             20.0.0.0/24     C
yes
20.0.0.2        vlan20         no             20.0.0.2/32     C
yes

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim neighbor

`show ip pim neighbor [<IP-ADDRESS>] [brief | all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
brief	Specifies PIM neighbor information display in brief format.
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM neighbor information for the 5420, 6200, 6300, 6400, 8100, 8325, 8360, 9300/9300S, 10000 Switch series:

```
switch# show ip pim neighbor

PIM Neighbor

VRF                               : default
Total number of neighbors : 1
```

```

IP Address           : 30.1.1.3
Interface            : vlan30
Up Time (HH:MM:SS)   : 03:55:40
Expire Time (HH:MM:SS) : 00:01:23
DR Priority           : NA
Hold Time (HH:MM:SS) : 00:01:45
Bidir Capable        : True

```

Showing PIM neighbor information in brief for the default VRF:

```

switch# show ip pim neighbor brief
-----
-
VRF: default                               Total number of neighbor : 2
-----
-
Interface  Neighbor  Uptime    Expires    DR          Hold Time  Secondary
Address    (IPv4)    (HH:MM:SS) (HH:MM:SS) Priority    (HH:MM:SS) (IPv4)
-----
-
29091/1/1  40.0.0.5  11:54:21  00:01:31   NA          00:01:45   Nil
29101/1/2  50.0.0.5  00:03:23  00:01:23   NA          00:01:45
60.0.0.4,70.0.0.4-----
-----

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Added support for BIDIR PIM on the 6200, 6300, 6400,8100, 8325, 8360, 9300, 10000 Switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

state-refresh-interval

```

state-refresh <INTERVAL-VALUE>
no state-refresh

```

Description

Configures the interval between successive state-refresh messages originated by the routing switch. Only the routing switch connected directly to the multicast source initiates state-refresh packets. All other PIM routers in the network only propagate these state-refresh packets.

The **no** form of this command sets the interval to the default value of 60 seconds.

Parameter	Description
<code><INTERVAL-VALUE></code>	Specifies the state refresh interval in seconds. Default: 60 seconds. Range 10-100.

Examples

Configuring the state refresh interval:

```
switch(config)# router pim
switch(config-pim)# state-refresh 30
switch(config-pim)# no state-refresh
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

Chapter 90

PIM-DM commands for IPv6

```
disable
```

disable

Description

Disables PIMv6 globally on the router.



Using the **disable** command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables PIMv6 globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim6  
switch(config-pim6)# enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense

```
ipv6 pim6-dense {enable | disable}  
no ipv6 pim6-dense [enable]
```

Description

Enables or disables PIM-DM on the current interface. PIM-DM is disabled by default on an interface. An IPv6 address must be configured on the interface to enable PIM-DM.

Parameter	Description
enable	Enables PIM-DM on the interface. IPv6 address must be configured on the interface to enable PIM-SM (use the ipv6 address <X:X::X:X/M> command).
disable	Disables PIM-DM on the interface.

Examples

Enabling and disabling PIM-DM on an interface:

```
switch(config)# interface vlan40  
switch(config-if-vlan)# ipv6 address 2001::01/64  
switch(config-if-vlan)# ipv6 pim6-dense enable  
switch(config-if-vlan)# ipv6 pim6-dense disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense bfd

```
ipv6 pim6-dense bfd [disable]
no ipv6 pim6-dense bfd
```

Description

Configures BFD on a per-interface basis for an interface associated with the PIM process.

The **no** form of this command removes the BFD configuration on the interface and sets it to the default configuration.



If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the **ipv6 pim6-dense bfd disable** command.

If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the **ipv6 pim6-dense bfd** command.

Parameter	Description
disable	Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense bfd
```

Disabling the BFD configuration on the interface:

```
switch(config-if-vlan)# ipv6 pim6-dense bfd disable
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ipv6 pim6-dense bfd
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense graft-retry-interval

```
ipv6 pim6-dense graft-retry-interval <INTERVAL-VALUE>  
no ipv6 pim6-dense graft-retry-interval
```

Description

Configures the interval for which the routing switch waits for the graft acknowledgment from another router before resending the graft request.

The **no** form of this command removes the currently configured value and sets to the default of 3 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the interval the routing switch waits for the graft acknowledgment. Default: 3 seconds. Range: 1-10.

Usage

Graft packets result when a downstream router transmits a request to join a flow. The upstream router responds with a graft acknowledgment packet. If the graft acknowledgment is not received within the time period of the graft-retry-interval, it resends the graft packet.

Example

Configuring and removing dense graft retry interval:

```
switch(config)# interface vlan40  
switch(config-if-vlan)# ipv6 pim6-dense graft-retry-interval 5  
switch(config-if-vlan)# no ipv6 pim6-dense graft-retry-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense hello-delay

```
ipv6 pim6-dense hello-delay <DELAY-VALUE>
no ipv6 pim6-dense hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The **no** form of this command removes currently configured value and sets to the default of 5 seconds.

Parameter	Description
<DELAY-VALUE>	Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Default: 5 seconds. Range: 0-5.

Usage

- In cases where a new interface activates connections with multiple routers, if all the connected routers sent hello packets at the same time, the receiving router could become momentarily overloaded.
- This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense hello-delay 4
switch(config-if-vlan)# no ipv6 pim6-dense hello-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense hello-interval

```
ipv6 pim6-dense hello-interval <INTERVAL-VALUE>
no ipv6 pim6-dense hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface. The **no** form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the frequency at which PIM Hello messages are transmitted on this interface. Default: 30 seconds. Range: 5-300.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing dense hello-interval:

```
switch(config)# interface 1/1/4
switch(config-if)# ipv6 pim6-dense hello-interval 60
switch(config-if)# no ipv6 pim6-dense hello-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense ipv6-addr

```
ipv6 pim6-dense ipv6-addr {<IPv6-ADDR-VALUE> | any}  
no ipv6 pim6-dense ipv6-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM packets sent from the interface or to use the specific IP address.

The **no** form of this command removes the currently configured value and sets to the default of **any**.

Parameter	Description
<IPv6-ADDR-VALUE>	Specifies an IPv6 address as the source IP for the interface.
any	Specifies dynamically determining the source IP from the current IPv6 address of the interface.

Examples

Configuring and removing the source IP address:

```
switch(config)# interface vlan40  
switch(config-if-vlan)# ipv6 pim6-dense ip-addr 2001::02  
switch(config-if-vlan)# no ipv6 pim6-dense ipv6-addr
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense lan-prune-delay

```
ipv6 pim6-dense lan-prune-delay  
no ipv6 pim6-dense lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default status is enabled. The **no** form of this command disables the LAN prune delay option.

Usage

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan40  
switch(config-if-vlan)# ipv6 pim6-dense lan-prune-delay  
switch(config-if-vlan)# no ipv6 pim6-dense lan-prune-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense max-graft-retries

```
ipv6 pim6-dense max-graft-retries <ATTEMPT-VALUE>
no ipv6 pim6-dense max-graft-retries
```

Description

Configures the number of attempts the routing switch will retry sending the same graft packet to join a flow.

The **no** form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameter	Description
<INTERVAL-VALUE>	Specifies the number of retries for the routing switch to resend the graft packet. Default: 3 attempts. Range: 1-10.

Usage

If a graft acknowledgment response is not received after the specified number of retries, the routing switch ceases trying to join the flow. In this case the flow is removed until either a state-refresh from upstream re-initiates the flow or an upstream router floods the flow. Increasing this value helps to improve multicast reliability.

Example

Configuring and removing the dense graft retry interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense max-graft-retries 6
switch(config-if-vlan)# no ipv6 pim6-dense max-graft-retries
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense override-interval

```
ipv6 pim6-dense override-interval <INTERVAL-VALUE>
no ipv6 pim6-dense override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The **no** form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameter	Description
<code><INTERVAL-VALUE></code>	Specifies the override interval of a LAN Prune Delay option in ms. Default: 2500 ms. Range: 500-6000.

Usage

Each router on the LAN expresses its view of the amount of randomization necessary in the Override Interval field of the LAN Prune Delay option. When all routers on a LAN use the LAN Prune Delay Option, all routers on the LAN MUST set their Override_Interval to the largest Override value on the LAN.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense override-interval 4000
switch(config-if-vlan)# no ipv6 pim6-dense override-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense propagation-delay

```
ipv6 pim6-dense propagation-delay <DELAY-VALUE>
no ipv6 pim6-dense propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The **no** form of this command removes currently configured value and sets to the default of 500 ms.

Parameter	Description
<code><DELAY-VALUE></code>	Specifies the propagation delay value in ms. Default: 500 ms. Range: 250-2000.

Usage

The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the link. When all routers on a link use the LAN Prune Delay Option, all routers on the LAN MUST set Propagation Delay to the largest LAN Delay on the LAN.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense propagation-delay 400
switch(config-if-vlan)# no ipv6 pim6-dense propagation-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense ttl-threshold

```
ipv6 pim6-dense ttl-threshold <THRESHOLD-VALUE>
no ipv6 pim6-dense ttl-threshold
```

Description

Configures the multicast datagram time-to-live (router hop-count) threshold for the interface. Any IP multicast datagrams or state-refresh packets with a TTL less than this threshold will not be forwarded out the interface.

The **no** form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameter	Description
<THRESHOLD-VALUE>	Specifies the time-to-live threshold. Default: 3 attempts. Range: 0-255.

Usage

The VLAN connected to the multicast source does not receive state refresh packets and thus is not state-refresh capable. Downstream VLANs in the switches are state-refresh capable. This parameter provides a method for containing multicast traffic within a network, or even within specific areas of a network. Initially, the multicast traffic source sets a TTL value in the packets it transmits. Each time one of these packets passes through a multicast routing device, the TTL setting decrements by 1. If the packet arrives with a TTL lower than the ttl-threshold, the routing switch does not forward the packet. The following aspects of the TTL setting of incoming multicast packets must be considered, before changing this parameter on a routing switch:

- A value that is too high will allow multicast traffic to go beyond the internal network.
- A value that is too low may prevent some intended hosts from receiving the desired multicast traffic.
- A value of 0 will forward multicast traffic regardless of the packet TTL setting.

Example

Configuring and removing the time-to-live threshold:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense ttl-threshold 8
switch(config-if-vlan)# no ipv6 pim6-dense ttl-threshold
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

no ipv6 pim6-dense

no ip pim-dense

Description

Removes PIM-DM for all IPv6 related configurations for the interface.

Examples

Removing all PIM-DM configurations on an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-dense
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

register-source

```
register-source <INTERFACE-NAME>
no register-source <INTERFACE-NAME>
```

Description

Specifies the source interface to be used for PIM registration in the case of VXLAN anycast interfaces. When the PIM enabled anycast VLAN is directly connected to a multicast source, **register-source** is used to send registration messages to the RP and this interface receives the register-stop messages from the RP.

The **no** form of this command removes the register source configuration.



For PIMv6, both IPv6 link-local and active-gateway address of the anycast VLAN interface is configured with the anycast link-local address. Refer to **EVPN VXLAN distributed anycast gateway** in the Multicast Guide for more information.

Parameter	Description
<INTERFACE-NAME>	Specifies the name of the interface to use.

Usage

- This is a global configuration under router-pim configuration and is required in Symmetric IRB with anycast IP address configuration.
- This configuration is required in the source connected switch only when the PIM-DR and RP are in two different switches.
- Without this configuration, there will be traffic loss as the registration sequence will not be successful. It is mandatory to have this source interface configured with a non-anycast IP address which is unique to the VTEP, and with PIM enabled.

Examples

Configuring the source interface for PIM registrations:

```
switch# config
switch(config)# router pim6 vrf vrf1
switch(config-pim)# register-source loopback1
```

Removing the **register-source** configuration:

```
switch(config-pim)# no register-source loopback1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced for PIMv6.
10.09.1000	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

router pim6

```
router pim6 [vrf <VRF-NAME>]
no router pim6 [vrf <VRF-NAME>]
```

Description

Changes the current context to the PIMv6 configuration context. If no VRF is specified, the default VRF is assumed.

The **no** form of this command removes the PIM configuration from the specified context or the default VRF.

Parameter	Description
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Examples

Configuring default router PIM:

```
switch(config)# router pim6
switch(config-pim6)#
```

Configuring specified router PIM:

```
switch(config)# router pim6 vrf Green
switch(config-pim6)#
```

Removing router PIM:

```
switch(config)# no router pim6
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

show ipv6 pim6

```
show ipv6 pim6 [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.

Parameter	Description
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 PIM router:

```
switch# show ipv6 pim6

PIM Global Parameters

VRF                : default
PIM Status          : Enabled
Join/Prune Interval (sec) : 46
SPT Threshold       : Disabled
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface

`show ipv6 pim6 interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>all-vrfs</code>	Optional. Shows mroute information for the group for all VRFs.
<code>vrf <VRF-NAME></code>	Optional. Shows mroute information for the group for a particular

Parameter	Description
	VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface:

```
switch# show ipv6 pim6 interface
PIM Interfaces

VRF: default

Interface      IP Address
mode
-----
1/1/1          fe80::a00:9ff:feec:dc0e/64
dense
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface <INTERFACE-NAME>

```
show ipv6 pim6 interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Parameter	Description
<INTERFACE-NAME>	Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface information for interface 1/1/1:

```
switch# show ipv6 pim6 interface 1/1/1

PIM Interfaces

VRF: default

Interface           : 1/1/1
IPv6 Address        : fe80::a00:9ff:feec:dc0e/64
Mode                 : dense

Designated Router   : fe80::a00:9ff:febd:8364
Hello Interval      : 30 sec
Hello Delay         : 4 sec

Override Interval   : 500 msec
Propagation Delay   : 350 msec
Neighbor Timeout    : 0
Graft Retry Interval : 9

LAN Prune Delay     : Yes
DR Priority          : 3
TTL Threshold       : 250
Max Graft Retries   : 9
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rpf

show ipv6 pim6 rpf [<IP-ADDRESS>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Displays PIM RPF details for the specified source or RP address in the given VRF and shows the nexthop and interface through which the shortest path to the source is available. It also displays if a PIM neighbor is present on the nexthop. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code><IP-ADDRESS></code>	Optional. Specifies an IP address in IPv6 format (xxxx:xxx:xxx:xxx:xxx:xxx:xxx:xxx), where x is a hexadecimal number from 0 to F. Shows PIM RPF details for the given IP address.
<code>all-vrfs</code>	Optional. Shows PIM interface information for all VRFs.
<code>vrf <VRF-NAME></code>	Optional. Shows PIM interface information for a particular VRF. If the <VRF-NAME> is not specified, it shows the default VRF information.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing PIM RPF information for the VRF named 'red':

```
switch# show ipv6 pim6 rpf vrf red
Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
O - OSPF, B - BGP, R - RIP
VRF: red
IP Address      : 2000::2
RPF Interface   : vlan20
RPF Nexthop     :
RPF Route/Mask  : 2000::2/128
Origin          : C
In Use          : yes
IP Address      : 2222::2
RPF Interface   : vlan20
RPF Nexthop     : fe80::94f1:2880:141d:a800 (PIM Neighbor)
RPF Route/Mask  : 2222::2/128
Origin          : O
In Use          : yes
```

Showing PIM RPF information for the specified IP address:

```
switch# show ipv6 pim6 rpf 2222::2 vrf red
Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
O - OSPF, B - BGP, R - RIP
VRF: red
IP Address      : 2222::2
RPF Interface   : vlan20
RPF Nexthop     : fe80::94f1:2880:141d:a800 (PIM Neighbor)
RPF Route/Mask  : 2222::2/128
Origin          : O
In Use          : yes
```

Showing PIM RPF information for all VRFs:

```
switch# show ipv6 pim6 rpf all-vrfs
Multicast RPF Details

Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
               O - OSPF, B - BGP, R - RIP

VRF: default
IP Address      : 1001::2
RPF Interface    : vlan10
RPF Nexthop      :
RPF Route/Mask   : 1001::2/128
Origin           : C
In Use           : yes

IP Address      : 1111::1
RPF Interface    : vlan10
RPF Nexthop      : fe80::94f1:2880:a1d:a800 (PIM Neighbor)
RPF Route/Mask   : 1111::1/128
Origin           : O
In Use           : yes

VRF: red
IP Address      : 2000::2
RPF Interface    : vlan20
RPF Nexthop      :
RPF Route/Mask   : 2000::2/128
Origin           : C
In Use           : yes

IP Address      : 2222::2
RPF Interface    : vlan20
RPF Nexthop      : fe80::94f1:2880:141d:a800 (PIM Neighbor)
RPF Route/Mask   : 2222::2/128
Origin           : O
In Use           : yes
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute

```
show ipv6 mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IPv6 mroute information for the default VRF:

```
Switch# show ipv6 mroute
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : ff32::10
Source Address     : fd00:192:168:20::2
SSM Mroute        : True
Neighbor           : fe80::f403:4301:1422:2600
Uptime            : 00:14:05
State              : route
Incoming interface : 1/1/5
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding
```

Showing IPv6 mroute information for all VRFs:

```
switch# do show ipv6 mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : ff32::10
Source Address     : fd00:192:168:2::100
SSM Mroute        : True
Neighbor           : fe80::eceb:b801:14e4:2900
Uptime            : 00:19:20
State              : route
Incoming interface : 1/1/4
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding

VRF : red
```

```

Total number of entries : 1

Group Address      : ff32::11
Source Address     : 30::3
SSM Mroute         : True
Neighbor           : fe80::eceb:b880:1fe4:2900
Uptime             : 00:01:13
State              : route
Incoming interface : vlan31
Outgoing Interface List :
Interface          State
-----
vlan32             forwarding

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute brief

```
show ipv6 mroute brief [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows mroute information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 mroute brief:

```

switch# show ipv6 mroute brief all-vrfs
IP Multicast Route Entries

VRF : blu
Total number of entries : 2

Group Address : ff08::1:3
Source Address : 2002::04
Neighbor      : 2003::04
Interface     : 1/1/2

Group Address : ff08::1:4
Source Address : 2002::03
Neighbor      : 2003::05
Interface     : 1/1/3

VRF : default
Total number of entries : 1

Group Address : ff08::1:5
Source Address : 2001::03
Neighbor      : 2002::01
Interface     : 1/1/1

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute <GROUP-ADDR>

```

show ipv6 mroute <GROUP-ADDR> [<SOURCE-ADDR>]
                        [all-vrfs | vrf <vrf-name>] [vsx-peer]

```

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<GROUP-ADDR>	Specifies show information for the group address. Format: X:X::X:X

Parameter	Description
<SOURCE-ADDR>	Optional. Specifies show information for the group from this source. Format: X:X::X:X
all-vrfs	Optional. Shows mroute information for the group for all VRFs.
vrf <VRF-NAME>	Optional. Shows mroute information for the group for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group ff08::1:3 and VRF green:

```
switch# show ipv6 mroute ff08::1:3 vrf green

IP Multicast Route Entries

VRF : green

Group Address           : ff08::1:3
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming Interface      : 1/1/1
Multicast Routing Protocol : PIM-DM
Unicast Routing Protocol : connected
Metric                  : 0
Metric Pref              : 0

Downstream Interface
Interface      State
-----
1/1/4          pruned
```

Showing information for group ff08::1:3 from source 2001::03 and all VRFs:

```
switch# show ipv6 mroute ff08::1:3 2001::03 all-vrfs

IP Multicast Route Entries

VRF : blue

Group Address           : ff08::1:3
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming Interface      : 1/1/1
Multicast Routing Protocol : PIM-DM
Unicast Routing Protocol : connected
Metric                  : 0
Metric Pref              : 0

Downstream Interface
Interface      State
```



```

-----      -----
1/1/4        pruned

VRF : green

Group Address      : ff08::1:3
Source Address     : 2001::03
Neighbor           : 2003::04
Incoming Interface : 1/1/2
Multicast Routing Protocol : PIM-DM
Unicast Routing Protocol : connected
Metric             : 0
Metric Pref        : 0

Downstream Interface
Interface          State
-----          -----
1/1/4              pruned

VRF : red

Group Address      : ff08::1:6
Source Address     : 2001::04
Neighbor           : 2003::04
Incoming Interface : 1/1/2
Multicast Routing Protocol : PIM-DM
Unicast Routing Protocol : connected
Metric             : 0
Metric Pref        : 0

Downstream Interface
Interface          State          By_Proxy_Dr
-----          -----          -----
vlan10            forwarding      false

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 neighbor

show ipv6 pim6 neighbor [<IPv6-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<IPv6-ADDR>	Specifies a neighbor address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM neighbor information:

```
switch# show ipv6 pim6 neighbor

PIM Neighbor

VRF                : default
IP Address         : 2001::02
Interface          : 1/1/1
Up Time (sec)      : 0
Expire Time (sec)  : 0
DR Priority         : 44
```

Showing PIM neighbor information (including the presence of anycast neighbors) for all VRFs:

```
switch# show ipv6 pim6 neighbor all-vrfs

PIM Neighbor

VRF                : red
Total number of neighbors : 2

IPv6 Address       : fe80::5:5:5:5
Interface          : vni10000
Up Time (HH:MM:SS) : 06:57:07
Expire Time (HH:MM:SS) : 00:03:26
DR Priority         : 1
Hold Time (HH:MM:SS) : 00:03:30

IPv6 Address       : fe80::3821:c780:a5c:18c0
Interface          : vlan10
Up Time (HH:MM:SS) : 00:01:46
Expire Time (HH:MM:SS) : 00:01:29
DR Priority         : 1
Hold Time (HH:MM:SS) : 00:01:45
Secondary IP Addresses :100:100::3
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

state-refresh-interval

```
state-refresh <INTERVAL-VALUE>
no state-refresh
```

Description

Configures the interval between successive state-refresh messages originated by the routing switch. Only the routing switch connected directly to the unicast source initiates state-refresh packets. All other PIM routers in the network only propagate these state-refresh packets.

The **no** form of this command sets the interval to the default value of 60 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the state refresh interval in seconds. Default: 60 seconds. Range 10-100.

Examples

Configuring the state refresh interval:

```
switch(config)# router pim6
switch(config-pim6)# state-refresh 30
switch(config-pim6)# no state-refresh
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

accept-register access-list

```
accept-register access-list <ACL-RULE>  
no accept-register access-list <ACL-RULE>
```

Description

Configures ACL on RP to filter PIM Register packets from unauthorized sources. The ACL specified will contain the (S,G) traffic in register packets to permitted or denied.

The **no** form of this command removes the currently configured ACL rule.

Parameter	Description
<ACL-RULE>	Specifies the ACL rule name.

Usage

When register ACL is associated with a PIM Router, PIM protocol will store the source and destination address details along with the action (permit or deny). If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Upon receiving the register messages, a look up is made to check if the S and G in the packet is in the permitted list. If there is no match or if there is a deny rule match, a register stop message is immediately sent and the packet is dropped and no further action is taken. Permitted packets will go through the normal flow.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Examples

Configuring ACL on RP with an ACL rule named **pim_reg_acl**:

```
switch(config)# access-list ip pim_reg_acl  
switch(config-acl-ip)# 10 permit any 20.1.1.1 225.1.1.2  
switch(config-acl-ip)# 20 deny any 30.1.1.1 225.1.1.3  
switch(config)# router pim  
switch(config-pim)# accept-register access-list pim_reg_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

accept-rp

```
accept-rp <IP-ADDR> access-list <ACL-RULE>
no accept-rp <IP-ADDR> access-list <ACL-RULE>
```

Description

Enables PIM router to filter PIM join/prune messages destined for a specific RP and specific groups. The ACL specifies the group addresses which are allowed or denied. Up to 8 RP addresses and group ACL can be associated with the PIM router.

The **no** form of this command removes the currently configured ACL rule.

Parameter	Description
<IP-ADDR>	Specifies the IPv4 address of the static RP. Format: A.B.C.D
<ACL-RULE>	Specifies the ACL rule name.

Usage

PIM will store the accepted RP address and the associated group ACL. When a join or prune message is received, a RP look up is made for the packet. If the RP is in the configured list and if the group in the join/prune packet is allowed in the ACL, the packet is allowed. Otherwise the packet is dropped.

To allow join/prune message from any groups, group address in the ACL can be wild-carded. In this case, only RP address check is performed.

This command impacts only (*,G) join/prune messages. If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.



If there is an active flow which is in the SPT, the traffic flow through the SPT will continue. Only (*,G) join/prune messages are dropped. (S,G) join/prune messages will not be impacted.

Examples

Configuring ACL on a RP with an ACL rule named **pim_rp_grp_acl** to filter join/prune messages:

```
switch(config)# access-list ip pim_rp_grp_acl
switch(config-acl-ip)# 10 permit any any 225.1.1.2/255.255.255.0
switch(config-acl-ip)# 20 permit any any 239.1.1.2/255.255.255.0
switch(config)-acl-ip# router pim
switch(config-pim)# accept-rp 30.1.1.1 access-list pim_rp_grp_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

active-active

active-active
no active-active

Description

Enables the PIM active-active mechanism per VRF on VSX. The default is disabled.

The **no** form of this command disables the PIM active-active mechanism.

Usage

PIM active-active keeps the multicast forwarding state synchronized on both VSX peer devices. Synchronization is achieved by electing the VSX peer that has the highest IP address as a designated router (DR) and the other as Proxy-DR.

If you want the multicast traffic to flow through VSX primary, assign higher IP addresses to the interfaces in VSX primary. When the VSX peer that is acting as the DR goes down, traffic is recovered faster since the multicast routes are synchronized.

Recommendations:

- Do not configure the DR priority of interfaces when **active-active** is enabled. The DR priority will be set to high on DR and default on Proxy-DR and any user-configured DR priority will be ignored.
- Always configure **keepalive** between VSX peers. If the ISL goes down when **keepalive** is not configured, both VSX peers start acting independently as DRs, resulting in duplicate traffic.
- Do not configure IGMP joins on transit VLANs.
- RP redundancy is not supported on the **active-active** mechanism. If one of the VSX peers is configured as RP and it goes down, the new traffic flows will not be converged until the RP is elected. For a static RP, new flows will never be converged until the VSX peer is back up.

Examples

Enabling the PIM active-active mechanism:

```
switch(config)# router pim  
switch(config-pim)# active-active
```

Disabling the PIM active-active mechanism:

```
switch(config)# router pim  
switch(config-pim)# no active-active
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

anycast-rp source-directly-connected

```
anycast-rp source-directly-connected  
[no] anycast-rp source-directly-connected
```

Description

Use this command with an Anycast rendezvous point (RP) solution (for example, with MSDP) when the same multicast source is directly connected to two or more Anycast RP routers.

Usage

When configured this command allows only one RP who is the Designated Router (DR) in the segment to own the generation of the MSDP SA (Source Active) messages. If this command is not enabled, all Anycast RP routers where the source is directly connected would start advertising SA messages and form a loop. For example, when the source is directly connected to an Anycast RP VSX pair via VSX-LAG. Therefore this configuration is recommended when VSX pairs act as Anycast RPs. This command is optional when the source is directly connected to a single Anycast RP router or when the source is at least one hop away from the RP.

Examples

The following examples configure directly connected sources with Anycast RP, then remove the configuration.


```
switch(config)# router pim
switch(config-pim)# anycast-rp source-directly-connected
switch(config-pim)#
switch(config-pim)# no anycast-rp source-directly-connected
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command Introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Users having admin privileges.

bfd all-interfaces

```
bfd all-interfaces
no bfd all-interfaces
```

Description

Enables BFD on all PIM interfaces. BFD can be disabled at individual PIM interface using the **ip pim-sparse bfd disable** command.

The **no** form of this command disables BFD for all the interfaces.

Examples

Enabling and disabling BFD on all PIM interfaces:

```
switch(config)# router pim
switch(config-pim)# bfd all-interfaces
switch(config-pim)# no bfd all-interfaces
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate bsm-interval

```
bsr-candidate bsm-interval <INTERVAL-VALUE>
no bsr-candidate bsm-interval
```

Description

Configures the interval in seconds to send periodic RP-Set messages to all PIM-SM interfaces on a router that operates as the BSR in a domain. This setting must be smaller than the **rp-candidate hold-time** settings (range of 30 to 255; default 150) configured in the RPs operating in the domain.

The **no** form of this command removes the currently configured value and sets it to the default of 60 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the BSR-candidate BSM interval in seconds. Default: 60 seconds. Range: 5-300.

Example

Configuring and removing BSR-candidate BSM-interval:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate bsm-interval 150
switch(config-pim)# no bsr-candidate bsm-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate hash-mask-length

```
bsr-candidate hash-mask-length <LENGTH-VALUE>
```

no bsr-candidate hash-mask-length

Description

Controls the distribution of multicast groups among the C-RP, in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) when allocating this distribution. A longer hash-mask-length results in fewer multicast groups, for each block of group addresses assigned to the RPs. Multiple blocks of addresses assigned to each C-RP results in wider dispersal of addresses. Includes enhanced load-sharing for the multicast traffic for the different groups that are used in the domain at the same time.

The **no** form of this command removes currently configured value and sets to the default of 30.

Parameter	Description
<LENGTH-VALUE>	Specifies the length (in bits) of the hash mask. Default: 30. Range: 1-32.

Example

Configuring and removing the BSR-candidate hash-mask-length:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate hash-mask-length 4
switch(config-pim)# no bsr-candidate hash-mask-length
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate priority

```
bsr-candidate priority <PRIORITY-VALUE>
no bsr-candidate priority
```

Description

Configures the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the BSR of the domain. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain.

The **no** form of this command removes currently configured value and sets to the default of 0.

Parameter	Description
<code><PRIORITY-VALUE></code>	Specifies the priority for the Candidate Bootstrap router. Default: 0. Range: 0-255

Example

Configuring and removing the BSR-candidate priority:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate priority 250
switch(config-pim)# no bsr-candidate priority
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate source-ip-interface

```
bsr-candidate source-ip-interface <INTERFACE-NAME>
no bsr-candidate source-ip-interface <INTERFACE-NAME>
```

Description

Configures the router to advertise itself as a candidate PIM-SM BSR on the interface specified, and enables BSR candidate operation. The result makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. One BSR candidate interface is allowed per-router.

The **no** form of this command removes the Candidate BSR configuration.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the interface to use as a source for Candidate-BSR router IP address. Interface can be a VLAN interface (such as vlan15) or routed interfaces (such as lag 1 or 1 / 1 / 19). PIM-SM must be enabled on this interface (use the ip pim-sparse enable command).

Example

Configuring and removing the BSR-candidate interface:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim)# bsr-candidate source-ip-interface vlan5
switch(config-pim)# no rp-candidate source-ip-interface 1/1/4
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables PIM globally on the router. PIM is disabled by default.



Using the **disable** command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim
switch(config-pim)# disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables PIM globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim
switch(config-pim)# enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

ip mroute

ip mroute <SRC-ADDR/SRC-MASK> <RPF-ADDRESS> | <INTERFACE-NAME>

Description

Configures multicast reverse path (RPF) forwarding static routes. This command is an alias of the **rpf-override** command.

Parameter	Description
<SRC-ADDR>	Specifies the multicast source address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<SRC-MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<RPF-ADDR>	Specifies the RPF address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<INTERFACE-NAME>	Specifies the RPF interface name.

Usage

Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.

Example

Configuring and removing an IP mroute:

```
switch(config)# router pim
switch(config-pim)# ip mroute 40.0.0.4/24 30.0.0.4
switch(config-pim)# no ip mroute 40.0.0.4/24 30.0.0.4
```

Configuring and removing an IP mroute for an IPv6 address:

```
switch(config-pim)# router pim6
switch(config-pim6)# ipv6 mroute 50::4/24 tunnel1
switch(config-pim6)# no ipv6 mroute 50::4/24 tunnel1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ip multicast boundary

```
ip multicast boundary access-list <acl_name>
no ip multicast boundary access-list <acl_name>
```

Description

This command configures administratively-scoped multicast boundaries on PIM-enabled Interfaces. A multicast boundary uses an Access Control List (ACL) to filter multicast traffic on the specified interface and prevent the routing of multicast traffic from that interface. This feature supports filtering based on IP, IGMP, and PIM protocols, and can filter both multicast data traffic and control packets, including **IGMP Join**, **PIM Join**, and **Prune** messages. The ACL can use the **any** filter to match traffic from any source to a specific IP multicast group (*,G), and can contain subnet masks to match a range of addresses.

Parameter	Description
access-list <acl_name>	Name of the boundary ACL to be applied on the interface.

Usage

When the multicast boundary is configured, MSDP is used to learn the multicast sources across the boundaries. Based on the ACL rules configured, the multicast traffic from one domain to other domain is permitted/denied. MSDP SA messages will always be forwarded across the boundaries regardless of multicast boundary ACL configurations. Anycast RP with MSDP mesh group across the boundaries is not supported. Multicast boundary feature is supported only for IPv4 currently. Multicast boundary feature is not supported on VXLAN based overlay networks.

Examples

The following example creates a boundary that denies multicast group IP addresses in 239.0.0.0/8 and permits group addresses in 224.0.0.0/4. Since the source address is **any**, it matches traffic from any multicast source (*,G).

```
access-list ip boundary1
 10 deny any any 239.0.0.0/255.0.0.0
 20 permit any any 224.0.0.0/240.0.0.0
interface vlan 40
 ip address 40.1.1.1/24
 ip pim-sparse enable
 ip multicast boundary access-list boundary1
```

The following example creates a boundary which permits traffic for specific multicast sources and groups IP addresses, and implicitly denies all other traffic.

```
access-list ip boundary2
 10 permit any 192.168.1.1 225.1.1.0/255.255.255.0
 20 permit any 172.168.1.1 239.1.1.0/255.255.255.0
interface vlan 40
 ip address 40.1.1.1/24
 ip pim-sparse enable
 ip multicast boundary access-list boundary2
```

The following boundary ACL creates a boundary based on protocols. The **PIM**, **IGMP**, and **IP** packets from the specified (S,G) are denied and all other traffic for 239.1.1.0/24 is allowed.


```

access-list ip boundary3
 30 deny pim 192.168.1.1 239.1.1.5
 40 deny igmp 192.168.1.1 239.1.1.5
 41 deny any 192.168.1.1 239.1.1.5
 50 permit any any 239.1.1.0/255.255.255.0
interface vlan 40
 ip address 40.1.1.1/24
 ip pim-sparse enable
 ip multicast boundary access-list boundary3

```

Related Commands

Command	Description
show ip multicast boundary interface	Displays IP Multicast boundary ACL configurations and packet drop counters for the given interface.



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip multicast multipath

```

ip multicast multipath {s-hash|s-g-hash}
no ip multicast multipath {s-hash|g-hash}

```

Description

This command configures the multipath hash mode, which allows the switch to determine the nexthop in the RPF path if there are multiple equal cost paths to a source address. PIM S,G join messages are sent to the selected nexthop which results in a multicast traffic flow in the selected paths. An even distribution of available nexthops across different multicast flows improves the utilization of ECMP paths.

Parameter	Description
s-hash	The hash to select the nexthop is based on only the source address. Flows originating from different sources will use different ECMP paths as the source is considered for selecting the nexthop.

Parameter	Description
	If the same source sends streams for multiple groups, then all the streams use only one of the ECMP paths. This is the default setting for this feature .
s-g-hash	This method uses both source and group address to select the nexthop. This allows better distribution of flows in scenarios where single source is streaming traffic for multiple groups.

Usage

Use this command only for route lookups for a source address and not for an Rendezvous Point (RP) address. The PIM *,G join messages which enable route lookup for the RP always uses the default **s-hash** mode, where nexthop is selected based on the RP IP address alone, and the group address is not part of the hash computation. Changes to the multipath has mode can result in traffic loss as the existing route cache is cleared and new route lookups are initiated. In topologies where PIM Assert messages are triggered, RPF lookups are not honored, and the packet forwarding path will be decided based on the assert winner.

Examples

Configuring the hash mode for an individual VRF:

```
switch(config)# vrf example
switch(config-vrf)# ip multicast multipath s-hash
```

Configuring the hash mode globally:

```
switch(config)# ip multicast multipath s-g-hash
```

Related Commands



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-vrf	Administrators or local user group members with execution rights for this command.

ip|ipv6 multicast rpf

```
ip multicast rpf select vrf <vrf-name> [group-prefix <grp-address/grp-mask>]
no ip multicast rpf select vrf <vrf-name> [group-prefix <grp-address/grp-mask>]
```

```
ipv6 multicast rpf select vrf <vrf-name> [group-prefix <grp6-address/grp-mask>]  
no ipv6 multicast rpf select vrf <vrf-name> [group-prefix <grp6-address/grp-mask>]
```

Description

Configures multicast route leaking to forward traffic from a source VRF to a receiver VRF by resolving Reverse Path Forwarding (RPF) lookup for multicast routes using unicast leaked routes. This command is configured under the receiver pim VRF context to specify the source VRF used for RPF.

Both dynamic and static RP configuration is supported with multicast IVRL. If static RP is configured, for any multicast traffic to be leaked from source VRF to the receiver VRF(s) it is mandated that static RP address is configured and associated with the group for which traffic leak is expected on both the source and receiver VRF routers. Also, static RP configuration is supported only in the source VRF not in any of the receiver VRFs for the leaked traffic. If the route-leaking device is acting as the RP for leaked traffic, it is recommended to use the RP address on Source VRF. Multicast route leaking is supported for up to 32 source VRFs.



Static RP (anycast/non-anycast) is supported in the source VRF only, but not in any of the receiver VRFs for the leaked traffic.

Unicast route leaking must be enabled on the multicast IVRL enabled router, and corresponding routes should be configured/advertised to the routers in the receiver VRF to ensure RP/source address reachability.

A single source VRF can be leaked into multiple client VRFs, for example IPTV. Multiple source VRFs can be leaked into single client VRF, for example (CCTV) but each source VRF should have a unique multicast group.



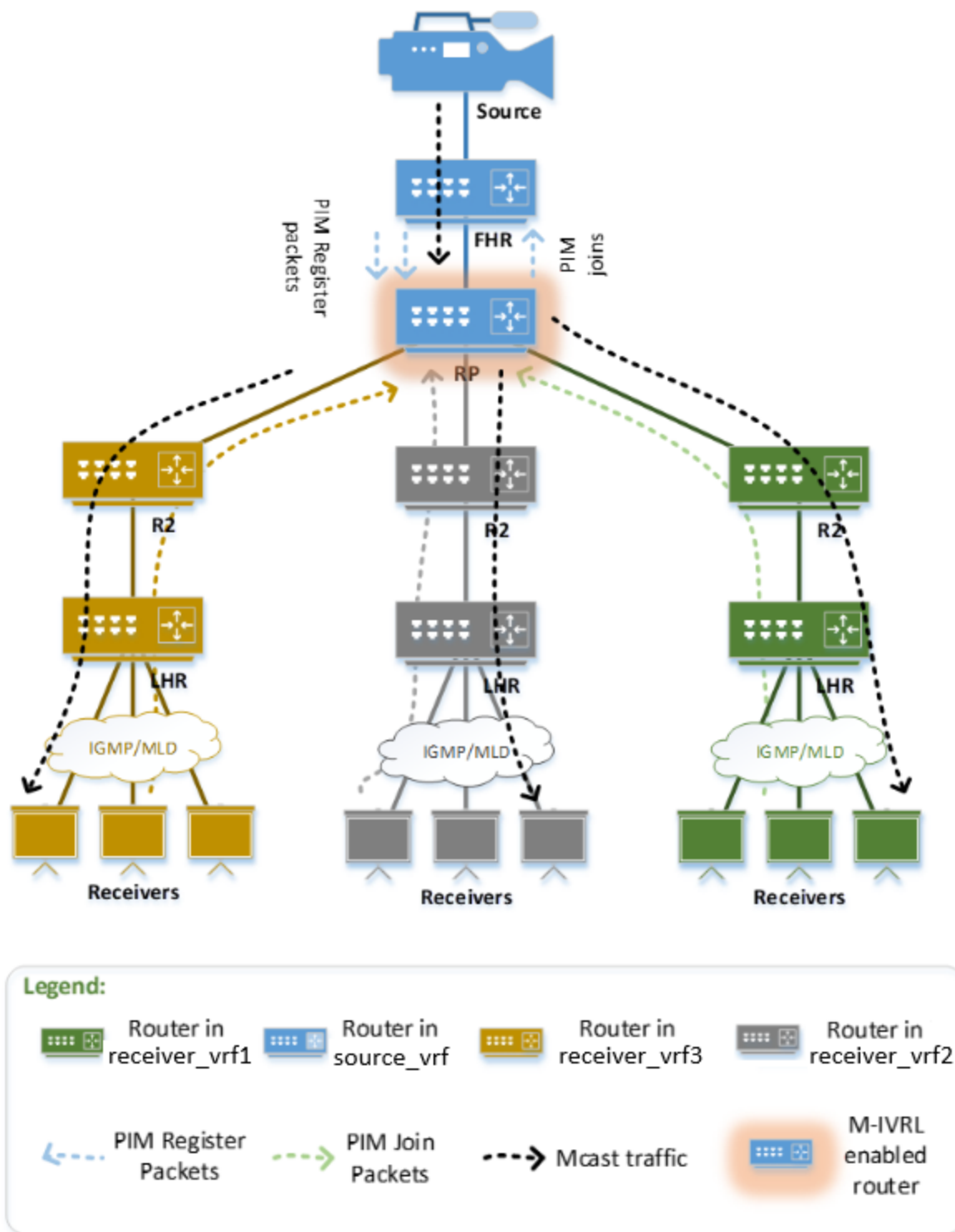
Do not configure route-leaking for the same group in a circular fashion, where VRF A leaks to VRF B, VRF B leaks to VRF C, and VRF C leaks traffic from VRF A for the same group. Multiple route-leak levels for the same group are not supported in the network. Cyclic leaks for the same group, such as VRF A to VRF B and VRF B to VRF A, are also not supported. If a VRF is configured as a source, it cannot act as a client VRF for multicast IVRL.

When IVRL is configured on a high scale setup, where the number of multicast routes are close to the MD scale for the platform, HPE Aruba Networking recommends increasing the PIM (v4) hello-interval to at least 60 seconds or more on all PIM enabled interfaces on each router in the topology. This will allow the IVRL device to recover faster from a network event like interface flap etc, without resulting in any neighbor fluctuations during the process.

Usage

Configure multicast route-leaking between VRF instances to achieve the following:

- Optimized multicast traffic forwarding in multi-vrf networks.
- Optimized hardware resource utilization.
- Traffic and service segregation.
- Flexible configuration/management.



The following configuration consistencies should be enforced on both the source and receiver VRFs:

- Static RP configuration for the leaked groups, including:
 - Static RP address.
 - Static RP group-range.
 - Static RP ACL.
- A multicast route leaking configuration on the VSX pair.

- An active-active configuration if the VSX pair device is configured for route leaking.
- Supported PIM-SM and PIM-SSM configurations.

For Dynamic RP functionality to operate correctly, MSDP must be enabled between all candidate RPs, as it facilitates RP-to-RP communication required for Dynamic RP operation:

- Any PIM enabled router can act as RP for source and client VRFs.
- Leaking device acts as RP for both client and source VRF.
- When 2 different devices act as RP for different VRFs, MSDP peering needs to be established between the two devices and sources has to be shared upto the client connected device.
- Mesh of MSDP peering need to be established between all Candidate-RPs to support RP failures.

Keep in mind the following with a multicast IVRL implementation:

- The rpf-override feature is mutually exclusive with multicast IVRL, as the RPF address won't correspond to a peer address in the VRF on which it's configured. Similarly, specifying a RPF interface requires a interface on another VRF which is not supported. Optimized hardware resource utilization.
- The ip mroute feature, where the RPF address/RPF interface is explicitly specified is also mutually exclusive with multicast IVRL since the RPF address won't correspond to a peer address in the VRF on which it's configured.
- Using the clear ip mroute feature with the group/group-range option is recommended to remove routes on IVRL enabled source VRFs.
- Using a multicast IVRL configuration in a VXLAN deployment is not supported in this release.

Recommended Best Practices for High-Scale IVRL Deployments:

When Inter-VRF Route Leaking (IVRL) is configured in a large-scale environment where the number of multicast routes approaches the platform's multi-dimensional (MD) scale or the VRF count is very high, the following best practices are strongly recommended:

1. **Increase the PIM Hello Interval:** Configure the PIM (IPv4/IPv6) hello-interval to 60 seconds or more on all PIM-enabled interfaces across all routers in the topology. This adjustment helps stabilize PIM neighbor relationships during transient events, such as interface flaps or link failures, allowing IVRL devices to recover more quickly without triggering unnecessary neighbor resets or route churn.
2. **Restrict Route Leaking to Specific Group Ranges:** Use the group-prefix command to leak only the required multicast groups, rather than using an open range. The overall processing load on the device is directly proportional to:
 - The number of multicast groups being leaked.
 - The number of VRFs to which these groups are leaked.

By restricting leakage to specific group ranges, you reduce the load on PIM and the control plane, and also prevent unintended traffic from being leaked between VRFs.



These measures help ensure that the network remains stable and efficient under high-scale IVRL scenarios—minimizing the risk of neighbor flaps, reducing unnecessary control-plane overhead, and maintaining predictable performance during recovery from network events.

Parameter	Description
<code><vrf-name></code>	Specifies the specific VRF name.

Parameter	Description
group-prefix	Specifies the multicast group address and mask.
grp6-addr/grp-mask	Specifies the multicast groupv6 address and mask.
no	Disables route leaking across VRFs for all group-ranges. Removes the IVRL configuration from the current VRF.

Examples

Enable multicast route leaking for specified VRF:

```
switch(config)# router pim vrf red
switch(config-pim)# ip multicast rp select vrf blue

Note: vrf(blue): source vrf and vrf (red): client vrf
```

Disable multicast route leaking for specified VRF:

```
switch(config-pim)# no ip multicast rp select vrf blue
```

To validate a route leak:

```
switch# show ip pim rp vrf red

Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
O - OSPF, B - BGP, R - RIP

VRF: red
IP Address RPF Interface RPF Nexthop PIM Neighbor RPF Route/Mask Origin In Use Egress VRF
-----
1.1.1.1    vlan10      10.1.1.1    yes          1.1.1.1/32    0      yes    blue
```

To show multicast route leak PIM global parameters:

```
Switch# show ip pim all-vrfs

PIM Global Parameters

VRF                : blue
PIM Status          : Enabled
PIM SSM Status      : Disabled
PIM SSM Range ACL   : Not Configured
Join/Prune Interval (sec) : 60
SPT Threshold       : Enabled
State Refresh Interval (sec) : 60
PIM NSF Status      : Inactive
PIM BIDI NSF Status : Inactive
Shared Border Status : Disabled
Multicast Fabric Identifier : 1
```

```

IVRL Status                : disbaled

VRF                        : red
PIM Status                 : Enabled
PIM SSM Status             : Disabled
PIM SSM Range ACL          : Not Configured
Join/Prune Interval (sec)  : 60
SPT Threshold              : Enabled
State Refresh Interval (sec) : 60
PIM NSF Status             : Inactive
PIM BIDI NSF Status        : Inactive
Shared Border Status       : Disabled
Multicast Fabric Identifier : 1
IVRL Status                : Enabled

```

To show IP multicast route entries:

```
switch# show ip mroute 225.1.1.1 all-vrfs detail
```

```
IP Multicast Route Entries
```

```
VRF      : blue
Total number of entries : 1
```

```

Group Address           : 225.1.1.1
Source Address          : 30.30.30.100
Neighbor                : 15.15.15.2
Incoming interface      : 1/1/11
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : OSPF
Metric                  : 200
Metric Pref              : 110
Uptime (HH:MM:SS)       : 00:05:05
Downstream Interface
Interface      State      Egress VRF
-----
1/1/12        forwarding   red

```

Command History

Release	Modification
10.17	The group-prefix and groupv6-prefix parameters were introduced.
10.15	Command introduced

Command Information

Platforms	Command context	Authority
9300	config-pim	Users are required to have administrative privileges to execute this command.

ip pim-sparse

```
ip pim-sparse {enable|disable}  
no ip pim-sparse [enable]
```

Description

Enables or disables PIM-SM in the current interface. PIM-SM is disabled by default on an interface. IP address must be configured on the interface to enable PIM-SM.

Parameter	Description
enable	Specifies PIM SM on the interface. IP address must be configured on the interface to enable PIM-SM.
disable	Disables PIM SM on the interface.

Examples

Enabling and disabling PIM-SM:

```
switch(config)# interface vlan 40  
switch(config-if-vlan)# ip address 40.0.0.4/24  
switch(config-if-vlan)# ip pim-sparse enable  
switch(config-if-vlan)# ip pim-sparse disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse bfd

```
ip pim-sparse bfd [disable]  
no ip pim-sparse bfd
```

Description

Configures BFD on a per-interface basis for one interface associated with the PIM process.

The **no** form of this command removes the BFD configuration on the interface and sets it to the default configuration.



If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the **ip pim-sparse bfd disable** command.

If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the **ip pim-sparse bfd** command.

Parameter	Description
disable	Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse bfd
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ip pim-sparse bfd
```

Disabling the BFD configuration on the interface and overriding the global setting:

```
switch(config-if-vlan)# ip pim-sparse bfd disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip pim-sparse bsr-boundary

```
ip pim-sparse bsr-boundary
no ip pim-sparse bsr-boundary
```

Description

Prevent exchange of PIM Bootstrap messages across multicast boundaries.

Usage

Best practices is to avoid exchanging PIM Bootstrap messages across different multicast domains as it will lead to election of RP in a different domain. When this command is configured on a boundary interface, PIM BSMs originating from other domain will be dropped and PIM BSMs originated within this domain will not forwarded to other domain. Note that this command will filter only PIM BSMs and is recommended to be enabled along with [ip multicast boundary](#).

Examples

Configuring and removing the BSR boundary:

```
switch(config-if)# interface 1/1/1
switch(config-if)# ip pim-sparse bsr-boundary
switch(config-if)# no ip pim-sparse bsr-boundary
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command Introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Users having admin privileges.

ip pim-sparse dr-priority

```
ip pim-sparse dr-priority <PRIORITY-VALUE>
no ip pim-sparse dr-priority
```

Description

Changes the router priority for the designated router (DR) election process in the current interface. A numerically higher value means a higher priority. If multiple routes share the highest priority, the router with the highest IP address is selected as the DR.

The **no** form of this command removes currently configured value and sets to the default of 1.

Parameter	Description
<PRIORITY-VALUE>	Specifies the priority value to use on the interface in the DR election process. Required. Default: 1. Range: 0- to 0-4294967295.

Examples

Configuring and removing the interface priority value:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse dr-priority 4444
switch(config-if-vlan)# no ip pim-sparse dr-priority
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse hello-delay

```
ip pim-sparse hello-delay <DELAY-VALUE>
no ip pim-sparse hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The **no** form of this command removes currently configured value and sets to the default of 5 seconds.

Parameter	Description
<DELAY-VALUE>	Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Default: 5. Range: 0 to 5.

Usage

- In cases where a new interface activates connections with multiple routers. If all the connected routers sent hello packets at the same time, the receiving router could become momentarily overloaded.
- This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse hello-delay 4
switch(config-if-vlan)# no ip pim-sparse hello-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse hello-interval

```
ip pim-sparse hello-interval <INTERVAL-VALUE>
no ip pim-sparse hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface. The **no** form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the frequency at which PIM Hello messages are transmitted on this interface. Range: 5 to 300. Default: 30.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.

- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing sparse hello-interval:

```
switch(config)# interface vlan 20
switch(config-if-vlan)# ip pim-sparse hello-interval 60
switch(config-if-vlan)# no ip pim-sparse hello-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse ip-addr

```
ip pim-sparse ip-addr {<IP-ADDR-VALUE> | any}
no ip pim-sparse ip-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM-SM packets sent from the interface or to use the specific IP address.

The **no** form of this command removes the currently configured value and sets to the default of **any**.

Parameter	Description
<IP-ADDR-VALUE>	Specifies an IP address as the source IP for the interface.
any	Specifies dynamically determining the source IP from the current IP address of the interface.

Examples

Configuring and removing source IP address:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse ip-addr 40.0.0.4
switch(config-if-vlan)# no ip pim-sparse ip-addr
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse lan-prune-delay

```
ip pim-sparse lan-prune-delay
no ip pim-sparse lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default is enabled.

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

The **no** form of this command disables the LAN prune delay option.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse lan-prune-delay
switch(config-if-vlan)# no ip pim-sparse lan-prune-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse override-interval

```
ip pim-sparse override-interval <INTERVAL-VALUE>
no ip pim-sparse override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The **no** form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameter	Description
<INTERVAL-VALUE>	Specifies the override interval of a LAN Prune Delay option in ms. Range: 500 to 6000. Default: 2500.

Usage

A router sharing a VLAN with other multicast routers uses the override-interval value along with the propagation-delay value to compute the **lan-prune-delay** setting. The setting specifies how long to wait for a PIM-SM join after receiving a prune packet from downstream for a particular multicast group.

Example scenario:

A network may have multiple routers sharing VLAN X. When an upstream router is forwarding traffic from multicast group X to VLAN Y, if one of the routers on VLAN Y does not want this traffic, it issues a prune response to the upstream neighbor. The upstream neighbor then goes into a prune pending state for group X on VLAN Y. During this period, the upstream neighbor continues to forward the traffic. During the pending period, another router on VLAN Y can send a group X join to the upstream neighbor. If this happens, the upstream neighbor drops the prune pending status and continues forwarding the traffic. But if no routers on the VLAN send a join, the upstream router prunes.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse override-interval 4000
switch(config-if-vlan)# no ip pim-sparse override-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ip pim-sparse propagation-delay

```
ip pim-sparse propagation-delay <DELAY-VALUE>
no ip pim-sparse propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The **no** form of this command removes currently configured value and sets to the default of 500 ms.

Parameter	Description
<DELAY-VALUE>	Specifies the propagation delay value in ms. Range: 250 to 2000. Default: 500.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse propagation-delay 400
switch(config-if-vlan)# no ip pim-sparse propagation-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 multicast rpf

```
ipv6 multicast rpf select vrf <vrf-name>
```

Description

Configure multicast route leaking to forward traffic from a source VRF to a receiver VRF by resolving Reverse Path Forwarding (RPF) lookup for multicast routes using unicast leaked routes. This command is configured under the receiver pim VRF context to specify the source VRF used for RPF.

Only a static RP configuration is supported with multicast IVRL. For multicast traffic to leak from the source VRF to receiver VRF(s), the static RP address must be configured and associated with the group the traffic leak is expected on for both the source and receiver VRF routers. If the route-leaking device is acting as the RP for leaked traffic, use the RP address on the source VRF. Multicast route leaking is supported for up to 8 source VRFs.



Static RP (anycast/non-anycast) is supported in the source VRF only, but not in any of the receiver VRFs for the leaked traffic.

Unicast route leaking must be enabled on the multicast IVRL enabled router, and corresponding routes should be configured/advertised to the routers in the receiver VRF to ensure RP/source address reachability.



A single source VRF can be leaked into multiple client VRFs, for example IPTV. Multiple source VRFs can be leaked into single client VRF, for example (CCTV) but each source VRF should have a unique multicast group.



Do not configure route-leaking in a circular fashion, where VRF A leaks from VRF B, VRF B leaks from VRF C, and VRF C leaks traffic from VRF A. Multiple route leak levels are not supported in the network. Cyclic leak (for multicast) VRF A to VRF B and VRF B to VRF A (reverse), is not supported. If VRF is configured as source, it cannot act as a client VRF for multicast IVRL.

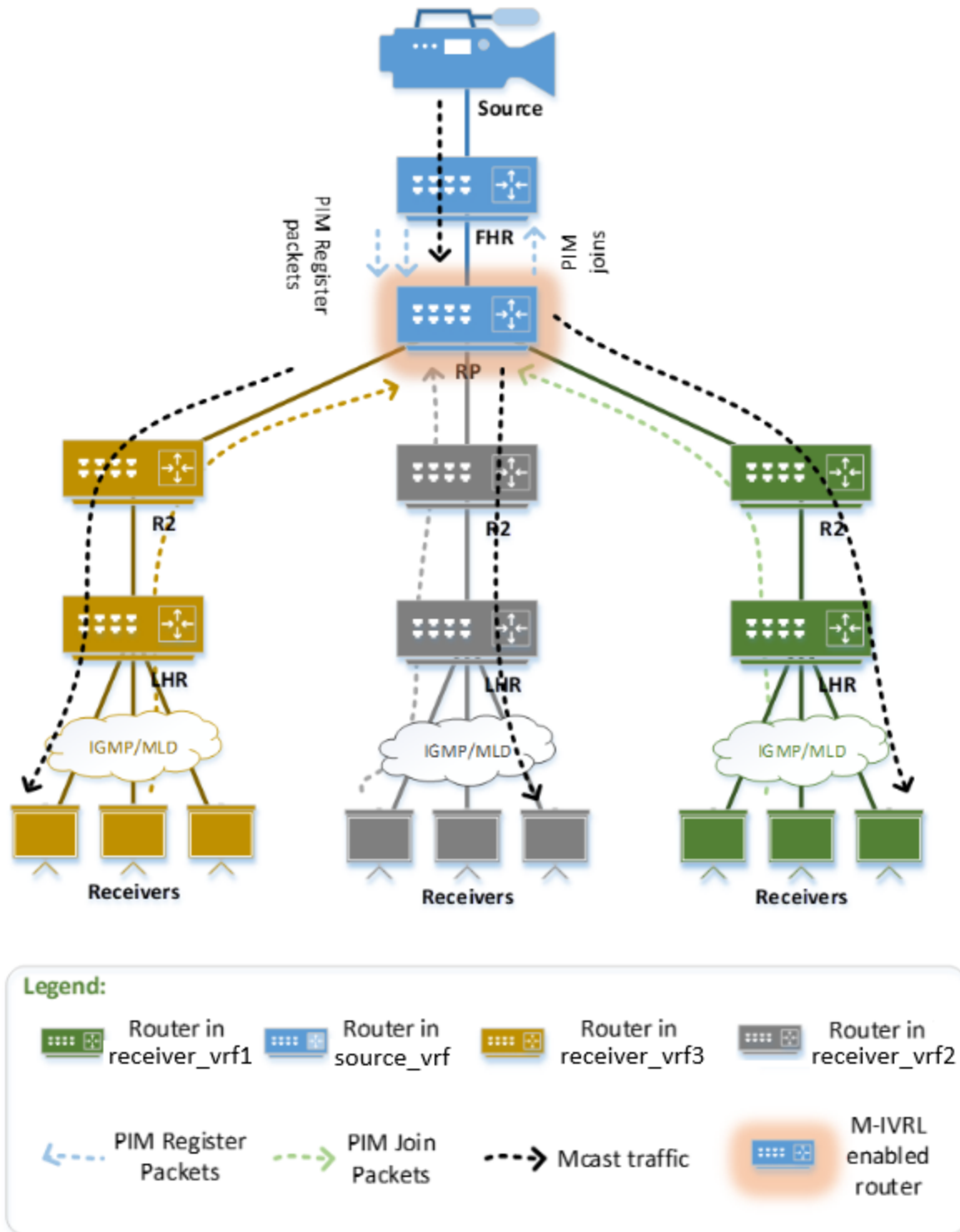


When IVRL is configured on a high scale setup, where the number of multicast route are close to the MD scale for the platform, HPE Aruba Networking recommends increasing the PIM (v6) hello-interval to at least 60 seconds or more on all PIM enabled interfaces on each router in the topology. This will allow the IVRL device to recover faster from a network event like interface flap etc, without resulting in any neighbor fluctuations during the process.

Usage

Configure multicast route-leaking between VRF instances to achieve the following:

- Optimized multicast traffic forwarding in multi-vrf networks
- Optimized hardware resource utilization
- Traffic and service segregation
- Flexible configuration/management



The following configuration consistencies should be enforced on both the source and receiver VRFs:

- Static RP configuration for the leaked groups, including:
 - Static RP address
 - Static RP group-range
 - Static RP ACL
- A multicast route leaking configuration on the VSX pair
- An active-active configuration if the VSX pair device is configured for route leaking
- Supported PIM-SM and PIM-SSM configurations

Keep in mind the following with a multicast IVRL implementation:

- The rpf-override feature is mutually exclusive with multicast IVRL, as the RPF address won't correspond to a peer address in the VRF on which it's configured. Similarly, specifying a RPF interface requires a interface on another VRF which is not supported. Optimized hardware resource utilization
- The ip mroute feature, where the RPF address/RPF interface is explicitly specified is also mutually exclusive with multicast IVRL since the RPF address won't correspond to a peer address in the VRF on which it's configured.
- Using the clear ip mroute feature with the group/group-range option is recommended to remove routes on IVRL enabled source VRFs.
- Using a multicast IVRL configuration in a VXLAN deployment is not supported in this release.

Parameter	Description
<code><vrf-name></code>	Specifies the specific VRF name.
<code><no></code>	Disables route leaking across VRFs for all group-ranges. Removes the IVRL configuration from the current VRF.

Examples

Enable multicast route leaking for specified VRF:

switch(config)# **router pim6 vrf red** switch(config-pim6)# **ipv6 multicast rpf select vrf blue** Note: vrf (blue): source vrf and vrf (red): client vrf

Disable multicast route leaking for specified VRF:

```
switch(config-pim6)# no ipv6 multicast rpf select vrf blue
```

To validate a route leak:

```
switch# show ipv6 pim rpf vrf red

Multicast RPF Details

Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
O - OSPF, B - BGP, R - RIP

VRF: red

IP Address : 5:5:5::5
RPF Interface : 1/1/3
RPF Nexthop : 10:10:10::2
```

```
PIM Neighbor : yes
RPF Route/Mask : 5:5:5::5/128
Origin : 0
In Use : yes
Egress VRF : blue
```

To show multicast route leak PIM global parameters:

```
Switch# show ipv6 pim6 all-vrfs

PIM Global Parameters

VRF                               : blue
PIM Status                       : Enabled
PIM SSM Status                   : Disabled
PIM SSM Range ACL                 : Not Configured
Join/Prune Interval (sec)        : 60
SPT Threshold                    : Enabled
State Refresh Interval (sec)     : 60
PIM NSF Status                   : Inactive
PIM BIDI NSF Status              : Inactive
Shared Border Status             : Disabled
Multicast Fabric Identifier       : 100
IVRL Status                      : Disbaled

VRF                               : red
PIM Status                       : Enabled
PIM SSM Status                   : Disabled
PIM SSM Range ACL                 : Not Configured
Join/Prune Interval (sec)        : 60
SPT Threshold                    : Enabled
State Refresh Interval (sec)     : 60
PIM NSF Status                   : Inactive
PIM BIDI NSF Status              : Inactive
Shared Border Status             : Disabled
Multicast Fabric Identifier       : 100
IVRL Status                      : Enabled
```

To show IP multicast route entries:

```
switch# show ipv6 mroute ff55::100:1 all-vrfs detail

IP Multicast Route Entries

VRF      : blue
Total number of entries : 1

Group Address           : ff55::100:1
Source Address          : 30.30.30::100
Neighbor                : fe80::b8d4:e701:38dd:d300
Incoming interface      : 1/1/3
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol  : OSPF
Metric                  : 200
Metric Pref              : 110
```

```
Uptime (HH:MM:SS)           : 00:02:05
Downstream Interface
Interface      State      Egress VRF
-----
1/1/5         forwarding   red
```

Command History

Release	Modification
10.15	Command introduced

Command Information

Platforms	Command context	Authority
9300	config-pim	Users are required to have administrative privileges to execute this command.

join-prune-interval

```
join-prune-interval <INTERVAL-VALUE>
no join-prune-interval
```

Description

Configures the frequency at which the router will send periodic join or prune-interval messages. The **no** form of this command sets the interval to the default value of 60 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the join-prune-interval in seconds. Range 5 to 65535 Default: 60.

Examples

Configuring join prune interval:

```
switch(config)# router pim
switch(config-pim)# join-prune-interval 400
switch(config-pim)# no join-prune-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

multicast-route-limit

```
multicast-route-limit <limit>  
no multicast-route-limit <limit>
```

Description

Configures the limit on the maximum number of multicast route entries that can be programmed. When the limit is configured, multicast route entries created because of IGMP or MLD membership reports, and multicast route entries created because of multicast streams are restricted to the configured limit.

The **no** form of this command removes the currently configured limit value.

Parameter	Description
<limit>	Specifies the value to be configured as the multicast route limit. Range: 1 to 4294967295.

Usage

Flows exceeding the configured multicast route limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration prevents creation of new multicast routes when limits are reached. At the time of configuration, if the device has more multicast routes than the configured limit, existing multicast routes continue to exist until they are removed.

The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage.

Examples

Configuring and removing the multicast route rate limit:

```
switch(config)# router pim  
switch(config-pim)# multicast-route-limit 1024  
switch(config-pim)# no multicast-route-limit
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

no ip pim-sparse

no ip pim-sparse

Description

Removes all the PIM-SM related configurations for the interface.

Example

Removing PIM-SM configuration:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# no ip pim-sparse
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

register-rate-limit

register-rate-limit <limit>
no register-rate-limit <limit>

Description

Configures the limit on the maximum number of register messages sent per second for every unique (S,G) entry. By default, there is no maximum rate set. When the limit is configured, register messages generation is limited to the configured value.

The **no** form of this command removes the currently configured limit value.

Parameter	Description
<code><limit></code>	Specifies the value to be configured as the register rate limit. Range: 1 to 4294967295.

Examples

Configuring and removing the register rate limit:

```
switch(config)# router pim
switch(config-pim)# register-rate-limit 10
switch(config-pim)# no register-rate-limit
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

register-source

```
register-source <INTERFACE-NAME>
no register-source <INTERFACE-NAME>
```

Description

Specifies the source interface to be used for PIM registration in the case of VXLAN anycast interfaces. When the PIM enabled anycast VLAN is directly connected to a multicast source, **register-source** is used to send registration messages to the RP and this interface receives the register-stop messages from the RP.

The **no** form of this command removes the register source configuration.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the name of the interface to use.

Usage

- This is a global configuration under router-pim configuration and is required in Symmetric IRB with anycast IP address configuration.

- This configuration is required in the source connected switch only when the PIM-DR and RP are in two different switches.
- Without this configuration, there will be traffic loss as the registration sequence will not be successful. It is mandatory to have this source interface configured with a non-anycast IP address which is unique to the VTEP, and with PIM enabled.

Examples

Configuring the source interface for PIM registrations:

```
switch# config
switch(config)# router pim vrf vrf1
switch(config-pim)# register-source loopback1
```

Removing the **register-source** configuration:

```
switch(config-pim)# no register-source loopback1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

router pim

```
router pim [vrf <VRF-NAME>]
  accept-register access-list <ACL-RULE>
  accept-rp <IP-ADDR> access-list <ACL-RULE>
  active-active
  bfd all-interfaces
  bsr-candidate {bsm-interval <INTERVAL-VALUE> | {hash-mask-length <LENGTH-VALUE> |
  priority <PRIORITY-VALUE> | source-ip-interface <INTERFACE-NAME>}}
  enable|disable
  join-prune-interval <INTERVAL-VALUE>
  multicast-route-limit <limit>
  no ...
  register-rate-limit <limit>
  rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
  rp-candidate {group-prefix <GRP-ADDR/GRP-MASK> |hold-time <TIME-VALUE> | priority
  <PRIORITY-VALUE> | source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-
  MASK>]]}
  rpf-override <SRC-ADDR/SRC-MASK><RPF-ADDR|INTERFACE-NAME>
```

Description

Changes the current context to the PIM configuration context and enables PIM globally on the router. If no VRF is specified, the default VRF is assumed.

The **no** form of this command removes the PIM configuration from the specified context or the default VRF.

Parameter	Description
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF.
<code>accept-register access-list <ACL-RULE></code>	Specify an ACL rule name to configures ACL on RP to filter PIM Register packets from unauthorized sources. The ACL specified will contain the (S,G) traffic in register packets to permitted or denied.
<code>accept-rp <IP-ADDR> access-list <ACL-RULE></code>	Specify the IPv4 address of the static RP and ACL rule name to enable the PIM router to filter PIM join/prune messages destined for a specific RP and specific groups. The ACL specifies the group addresses which are allowed or denied. Up to 8 RP addresses and group ACL can be associated with the PIM router. PIM will store the accepted RP address and the associated group ACL. When a join or prune message is received, a RP look up is made for the packet. If the RP is in the configured list and if the group in the join/prune packet is allowed in the ACL, the packet is allowed. Otherwise the packet is dropped. To allow join/prune message from any groups, group address in the ACL can be wild-carded. In this case, only RP address check is performed. This parameter impacts only (*,G) join/prune messages. If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL. Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements. When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received. NOTE: If there is an active flow which is in the SPT, the traffic flow through the SPT will continue. Only (*,G) join/prune messages are dropped. (S,G) join/prune messages will not be impacted.
<code>active-active</code>	Enables the PIM active-active mechanism per VRF on VSX. The default is disabled. PIM active-active keeps the multicast forwarding state synchronized on both VSX peer devices. Synchronization is achieved by electing the VSX peer that has the highest IP address as a designated router (DR) and the other as Proxy-DR. If you want the multicast traffic to flow through VSX primary, assign higher IP addresses to the interfaces in VSX primary. When the VSX peer that is acting as

Parameter	Description
	the DR goes down, traffic is recovered faster since the multicast routes are synchronized.
<code>bfd all-interfaces</code>	Enables BFD on all PIM interfaces. BFD can be disabled at individual PIM interface using the ip pim-sparse bfd disable command.
<code>bsr-candidate</code>	Configure settings for a router that operates as the BSR in a domain.
<code>bsm-interval <INTERVAL-VALUE></code>	Configures the interval in seconds to send periodic RP-Set messages to all PIM-SM interfaces on a router that operates as the BSR in a domain. This setting must be smaller than the rp-candidate hold-time settings (range of 30 to 255; default 150) configured in the RPs operating in the domain. Default: 60 seconds. Range: 5-300.
<code>hash-mask-length <LENGTH-VALUE></code>	Controls the distribution of multicast groups among the C-RP, in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) when allocating this distribution. A longer hash-mask-length results in fewer multicast groups, for each block of group addresses assigned to the RPs. Multiple blocks of addresses assigned to each C-RP results in wider dispersal of addresses. Includes enhanced load-sharing for the multicast traffic for the different groups that are used in the domain at the same time. Default: 30 bits. Range: 1-32.
<code>priority <PRIORITY-VALUE></code>	Configures the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the BSR of the domain. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain. Default: 0. Range: 0-255
<code>source-ip-interface <INTERFACE-NAME></code>	Configures the router to advertise itself as a candidate PIM-SM BSR on the interface specified, and enables BSR candidate operation. The result makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. One BSR candidate interface is allowed per-router. The Interface can be a VLAN interface (such as vlan15) or routed interfaces (such as lag 1 or 1 / 1 / 19). PIM-SM must be enabled on this interface (use the ip pim-sparse enable command).
<code>enable disable</code>	Enables or disables PIM globally on the router.

Parameter	Description
<code>join-prune-interval <INTERVAL-VALUE></code>	Configures the frequency at which the router will send periodic join or prune-interval messages. Range 5 to 65535 Default: 60.
<code>multicast-route-limit <limit></code>	Configures the limit on the maximum number of multicast route entries that can be programmed. When the limit is configured, multicast route entries created because of IGMP or MLD membership reports, and multicast route entries created because of multicast streams are restricted to the configured limit. Flows exceeding the configured multicast route limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration prevents creation of new multicast routes when limits are reached. At the time of configuration, if the device has more multicast routes than the configured limit, existing multicast routes continue to exist until they are removed. The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage. Range: 1 to 4294967295.
<code>no...</code>	Negates any configured parameter.
<code>register-rate-limit <limit></code>	Configures the limit on the maximum number of register messages sent per second for every unique (S,G) entry. By default, there is no maximum rate set. When the limit is configured, register messages generation is limited to the configured value. Range: 1 to 4294967295.
<code>rp-address</code>	Statically configures the router as the RP for a specified multicast group or range of multicast groups. When a static RP and a C-RP are configured to support the same multicast groups and the multicast group mask for the static RP is equal to or greater than the same mask for the applicable C-RPs, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a backup RP for the configured group. Without override, the C-RP has precedence over a static RP configured for the same multicast group or groups. This must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv4 multicast addresses (224.0.0.0 - 239.255.255.255). PIM-SM supports a maximum of 8 static RPs per VRF.
<code><IP-ADDR></code>	Specifies the address of the static RP in IPv4 format (x.x.x.x).
<code><GRP-ADDR/GRP-MASK></code>	Specifies the multicast group address in IPv4 format (x.x.x.x) and the address mask in CIDR format (x),

Parameter	Description
	where x is a decimal number from 0 to 128.
<code>override</code>	Specifies higher precedence to static RP over Candidate RP.
<code>rp-candidate</code>	Configure Candidate Rendezvous Point (C-RP) settings.
<code>group-prefix <GRP-ADDR/GRP-MASK></code>	Adds multicast group address to the current Candidate Rendezvous Point (C-RP) configuration by specifying the the multicast group address in IPv4 format (x.x.x.x) and the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code>hold-time <TIME-VALUE></code>	Changes the hold-time a C-RP includes in its advertisements to the BSR. Hold-time is included in the advertisements the C-RP periodically sends to the elected BSR for the domain. Also updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming it has become unavailable. Range: 30 to 250. Default: 150.
<code>priority <PRIORITY-VALUE></code>	Changes the current priority setting for a C-RP. Where multiple C-RP configurations are used to support the same multicast groups, the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority. Range: 0 to 255. Default: 192.
<code>source-ip-interface</code>	Enables the Candidate Rendezvous Point (C-RP) operation, and configures the router to advertise itself as a C-RP to the Bootstrap Router (BSR) for the current domain. This step includes the option to allow the C-RP to be a candidate for all possible multicast groups, or for up to four multicast groups, or ranges of groups. If group-prefix is not given, it considers for all multicast group addresses.
<code><INTERFACE-NAME></code>	Specifies the interface to use as a source for the C-RP router IP address.
<code>group-prefix <GRP-ADDR/GRP-MASK></code>	Specifies the multicast group address in IPv4 format (x.x.x.x) and the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code>rpf-override</code>	The Reverse Path Forward (RPF) override allows overriding the normal RPF lookup mechanism, and indicates to the router that it may accept multicast traffic on an interface other than the one that the RPF lookup mechanism would normally select. This includes accepting traffic from an invalid source IP address for the subnet or VLAN that is directly connected to the router. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received

Parameter	Description
	multicast traffic.
<SRC-ADDR/SRC-MASK>	Specifies the multicast source IPv4 address in IPv4 format (x.x.x.x) and the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<RPF-ADDR INTERFACE-NAME>	Specifies the RPF override IP address or interface.

Usage

When a register ACL is associated with a PIM Router, the PIM protocol will store the source and destination address details along with the action (permit or deny). If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Upon receiving the register messages, a look up is made to check if the S and G in the packet is in the permitted list. If there is no match or if there is a deny rule match, a register stop message is immediately sent and the packet is dropped and no further action is taken. Permitted packets will go through the normal flow.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Recommendations for the active-active mechanism:

- Do not configure the DR priority of interfaces when **active-active** is enabled. The DR priority will be set to high on DR and default on Proxy-DR and any user-configured DR priority will be ignored.
- Always configure **keepalive** between VSX peers. If the ISL goes down when **keepalive** is not configured, both VSX peers start acting independently as DRs, resulting in duplicate traffic.
- Do not configure IGMP joins on transit VLANs.
- RP redundancy is not supported on the **active-active** mechanism. If one of the VSX peers is configured as RP and it goes down, the new traffic flows will not be converged until the RP is elected. For a static RP, new flows will never be converged until the VSX peer is back up.

Reverse Path Forward (RPF) override usage details:

- Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.
- RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified. The RPF-address indicates one of two distinct RPF candidates:
 1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of **<source-addr/src-mask>**.
 2. A local router address on a PIM-enabled interface to which **<source-addr/src-mask>** is directly connected. If configured, the local router will assume the role of DR for this flow and registers the flow with an RP.

Examples

Configuring and enabling default router PIM:

```
switch(config)# router pim  
switch(config-pim)#enable
```

Configuring specified router PIM:

```
switch(config)# router pim vrf green  
switch(config-pim)#
```

Configuring ACL on RP with an ACL rule named **pim_reg_acl**:

```
switch(config)# access-list ip pim_reg_acl  
switch(config-acl-ip)# 10 permit any 20.1.1.1 225.1.1.2  
switch(config-acl-ip)# 20 deny any 30.1.1.1 225.1.1.3  
switch(config)# router pim  
switch(config-pim)# accept-register acces
```

Configuring ACL on a RP with an ACL rule named **pim_rp_grp_acl** to filter join/prune messages:

```
switch(config)# access-list ip pim_rp_grp_acl  
switch(config-acl-ip)# 10 permit any any 225.1.1.2/255.255.255.0  
switch(config-acl-ip)# 20 permit any any 239.1.1.2/255.255.255.0  
switch(config)-acl-ip# router pim  
switch(config-pim)# accept-rp 30.1
```

Configuring and removing the BSR-candidate interface:

```
switch(config)# router pim  
switch(config-pim)# bsr-candidate source-ip-interface 1/1/4  
switch(config-pim)# bsr-candidate source-ip-interface vlan5  
switch(config-pim)# no rp-candidate source-ip-interface 1/1/4
```

Configuring and removing the multicast route rate limit:

```
switch(config)# router pim  
switch(config-pim)# multicast-route-limit 1024  
switch(config-pim)# no multicast-route-limit
```

Configuring and removing the register rate limit:

```
switch(config)# router pim  
switch(config-pim)# register-rate-limit 10  
switch(config-pim)# no register-rate-limit
```

Configuring and removing candidate-RP router priority and hold times

```
switch(config)# router pim
switch(config-pim)# rp-candidate priority 250
switch(config-pim)# rp-candidate hold-time 200
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

rp-address

```
rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
no rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
```

Description

Statically configures the router as the RP for a specified multicast group or range of multicast groups. This must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv4 multicast addresses (224.0.0.0 - 239.255.255.255). PIM-SM supports a maximum of 8 static RPs per VRF. Optionally associates the specified access control list to the given static RP address.

The **no** form of this command removes static RP configuration and its precedence.

Parameter	Description
<IP-ADDR>	Specifies the address of the static RP in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<GRP-ADDR>	Specifies the multicast group address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<GRP-MASK>	Specifies the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
override	Specifies higher precedence to static RP over candidate RP.

Usage

Where a static RP and a C-RP are configured to support the same multicast groups and the multicast group mask for the static RP is equal to or greater than the same mask for the applicable C-RPs, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a

backup RP for the configured group. Without override, the C-RP has precedence over a static RP configured for the same multicast group or groups.

Examples

Configuring the static RP precedence over the candidate RP:

```
switch(config)# router pim
switch(config-pim)# rp-address 40.0.0.4 230.0.0.4/24 override
switch(config-pim)# rp-address 40.0.0.8 222.0.0.4/24
switch(config-pim)# no rp-address 40.0.0.4 230.0.0.4/24
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-address access list

```
rp-address <IP-ADDR> [access-list <ACL-NAME>][override]
no rp-address <IP-ADDR> [access-list <ACL-NAME>][override]
```

Description

Statically configures the router as the RP and associates the static RP to the specified ACL.

The **no** form of this command removes static RP ACL configuration.

Parameter	Description
<IP-ADDR>	Specifies the address of the static RP in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<i>access-list <ACL-NAME></i>	Specifies the name of the access control list.
override	Specifies whether or not static RP configuration precedes the information learned by a BSR.

Usage

The ACL includes a list of permitted/ denied group addresses for the specified RP.

- When configured on a source DR, only permitted group addresses are registered to the RP. When applied on other routers, (*,G) PIM join/prune messages are filtered according to the applied ACL.
- Only destination group addresses in the ACEs are filtered and any other fields configured in the ACE are ignored. If only PIM (*,G) messages need to be filtered, configure **accept-rp** ACLs.
- When static RP ACL is configured, only one static RP can be configured per VRF and that configured RP handles all the multicast groups in range 224.0.0.0/4.



A change in the RP ACL does not impact the flows that have already switched to SPT. Only when the source information is expired and the RP is needed to establish the multicast tree, is the change in the ACL reflected. If the source is always active, PIM can be disabled and re-enabled to clear the learned sources information and re-establish multicast trees based on the latest RP ACL configurations.

Examples

Configuring the static RP ACL:

```
...
access-list ip static_rp_acl
  10 permit any any 225.1.1.1
  20 permit any any 239.1.1.0/255.255.255.0
  30 deny any any 226.1.1.0/255.255.255.0

switch(config)# router pim
switch(config-pim)# rp-address 40.0.0.4 access-list static_rp_acl
```

Removing the static RP ACL configuration:

```
switch(config-pim)# no rp-address 40.0.0.4 access-list static_rp_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Added optional access list parameter [access-list <ACL-NAME>]
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate group-prefix

```
rp-candidate group-prefix <GRP-ADDR/GRP-MASK>
no rp-candidate group-prefix <GRP-ADDR/GRP-MASK>
```

Description

Adds multicast group address to the current Candidate Rendezvous Point (C-RP) configuration. The **no** form of this command removes C-RP multicast group address.

Parameter	Description
<code><GRP-ADDR></code>	Specifies the multicast group address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<code><GRP-MASK></code>	Specifies the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

Configuring and removing candidate group prefix:

```
switch(config)# router pim
switch(config-pim)# rp-candidate group-prefix 230.0.0.4/24
switch(config-pim)# no rp-candidate group-prefix 230.0.0.4/24
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate hold-time

```
rp-candidate hold-time <TIME-VALUE>
no rp-candidate hold-time
```

Description

Changes the hold-time a C-RP includes in its advertisements to the BSR.

Hold-time is included in the advertisements the C-RP periodically sends to the elected BSR for the domain. Also updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming it has become unavailable.

The **no** form of this command removes the currently configured value and sets it to the default value 150 seconds.

Parameter	Description
<code><TIME-VALUE></code>	Specifies the hold-time value in seconds to be sent in C-RP-Adv messages. Range: 30 to 250. Default: 150.

Example

Setting and removing the candidate holdtime:

```
switch(config)# router pim
switch(config-pim)# rp-candidate hold-time 250
switch(config-pim)# no rp-candidate hold-time
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate priority

```
rp-candidate priority <PRIORITY-VALUE>
no rp-candidate priority
```

Description

Changes the current priority setting for a C-RP. Where multiple C-RP configurations are used to support the same multicast groups, the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority.

The **no** form of this command removes the currently configured value and sets it to the default of 192.

Parameter	Description
<code><PRIORITY-VALUE></code>	Specifies the priority value for the Candidate-RP router. Range: 0 to 255. Default: 192.

Example

Configuring and removing candidate priority:

```
switch(config)# router pim
switch(config-pim)# rp-candidate priority 250
switch(config-pim)# no rp-candidate priority
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate source-ip-interface

```
rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
no rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
```

Description

Enables the Candidate Rendezvous Point (C-RP) operation, and configures the router to advertise itself as a C-RP to the Bootstrap Router (BSR) for the current domain.

This step includes the option to allow the C-RP to be a candidate for all possible multicast groups, or for up to four multicast groups, or ranges of groups. If group-prefix is not given, it considers for all multicast group addresses.

The **no** form of this command removes the C-RP configuration.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to use as a source for the C-RP router IP address.
<GRP-ADDR>	Specifies the multicast group address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<GRP-MASK>	Specifies the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

Configuring and removing candidate source IP interface:

```
switch(config)# router pim
switch(config-pim)# rp-candidate source-ip-interface vlan40 group-prefix
```

230.0.0.4/24

```
switch(config-pim)# no rp-candidate source-ip-interface vlan20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rpf-override

```
rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR| INTERFACE-NAME>
```

```
no rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR| INTERFACE-NAME>
```

Description

The Reverse Path Forward (RPF) override, allows overriding the normal RPF lookup mechanism, and indicates to the router that it may accept multicast traffic on an interface other than the one that the RPF lookup mechanism would normally select. This includes accepting traffic from an invalid source IP address for the subnet or VLAN that is directly connected to the router. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.

The **no** form of this command removes currently configured RPF entry.

Parameter	Description
<SRC-ADDR/SRC-MASK>	Specifies the multicast source IPv4 address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. And the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<RPF-ADDR>	Specifies the RPF address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<INTERFACE-NAME>	Specifies the RPF interface name.

Usage

Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source

address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.

Example

Configuring and removing RPF override:

```
switch(config)# router pim
switch(config-pim)# rpf-override 40.0.0.4/24 30.0.0.4
switch(config-pim)# no rpf-override 40.0.0.4/24 30.0.0.4
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

show ip mroute

```
show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows mroute information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP mroute for the default VRF:

```
Switch(config-vlan-20)# show ip mroute
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : 232.10.10.10
Source Address     : 192.168.20.2
SSM Mroute        : True
Neighbor          : 192.168.3.0
Uptime            : 02:08:31
State             : route
Incoming interface : 1/1/5
Outgoing Interface List :
Interface          State
-----
vlan20            forwarding
```

Showing IP mroute for all VRFs:

```
switch# do show ip mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : 232.10.10.10
Source Address     : 192.168.2.100
SSM Mroute        : True
Neighbor          : 192.168.3.0
Uptime            : 00:38:24
State             : route
Incoming interface : 1/1/4
Outgoing Interface List :
Interface          State
-----
vlan20            forwarding

VRF : red
Total number of entries : 1

Group Address      : 232.11.11.11
Source Address     : 30.0.0.3
SSM Mroute        : True
Neighbor          : 31.0.0.1
Uptime            : 00:32:55
State             : route
Incoming interface : vlan31
Outgoing Interface List :
Interface          State
-----
vlan32            forwarding

switch#
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute brief

```
show ip mroute brief [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows mroute information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IP mroute brief:

```
switch# show ip mroute brief
VRF : default
Total number of entries : 1

Group Address      Source Address      Neighbor      Interface
-----
239.1.1.1          40.0.0.6            10.1.1.2      vlan5
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute group-addr

```
show ip mroute <GROUP-ADDR> [<SOURCE-ADDR>] [all-vrfs | vrf <vrf-name>] [vsx-peer]
```

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<GROUP-ADDR>	Specifies a group address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<SOURCE-ADDR>	Specifies show information for the group from this source in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
all-vrfs	Shows mroute information for the group for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group 239.1.1.1 and VRF green:

```
switch# show ip mroute 239.1.1.1 vrf green

VRF : green

Group Address           : 239.1.1.1
Source Address          : 40.0.0.5
Neighbor                : 10.1.1.2
Incoming interface      : vlan1
Unicast Routing Protocol : connected
Metric                  : 1234
Metric Pref              : 1234
Downstream Interface
Interface   State
-----
vlan6      forwarding
```

Showing information for group 239.1.1.1 from source 40.0.0.5 and all VRFs:

```
switch# show ip mroute 239.1.1.1 40.0.0.5 all-vrfs
```

```

VRF : blue

Group Address          : 239.1.1.1
Source Address         : 40.0.0.5
Incoming interface     : vlan3
Unicast Routing Protocol : connected
Metric                 : 1234
Metric Pref            : 1234
Downstream Interface
Interface      State
-----
vlan2          forwarding

VRF : green

Group Address          : 239.1.1.1
Source Address         : 40.0.0.5
Neighbor              : 10.1.1.2
Incoming interface     : vlan1
Unicast Routing Protocol : connected
Metric                 : 1234
Metric Pref            : 1234
Downstream Interface
Interface      State
-----
vlan6          forwarding

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast anomalies

```

show ip multicast anomalies (pim | igmp | msdp | data-path | all) {source <source_ip>}
{group <group_ip>} {interface <IFNAME>} {vrf <vrf_name>} {all-vrfs}

```

Description

This command is used to display IPv4 multicast anomalies occurring across all the multicast modules in the system. Use this issue to troubleshoot current issues, or to detect multicast issues that occurred in the past by capturing the list of anomalies occurring across the multicast stack.

Parameter	Description
pim	Display multicast anomalies specific to PIM.
igmp	Display multicast anomalies specific to IGMP.
msdp	Display multicast anomalies specific to MSDP.
data-path	Display multicast anomalies specific to the datapath.
all	Display anomalies of all muticast modules.
group <group_ip>	Display multicast anomalies specific to the group.
interface <IFNAME>	Display multicast anomalies specific to an interface
source <source_ip>	Display multicast anomalies specific to a source.
vrf <vrf-name>	Display multicast anomalies specific to a VRF.
all-vrfs	Display multicast anomalies for all VRFs.

Examples

Showing datapath multicast anomalies for a specified group, interface and VRF.

```
switch# show ip multicast anomalies all all-vrfs

2022-02-18T09:28:40.272639+00:00 8320 pimd[2206]: MCAST_ANOMALY|IPV4|PIM|-
|100.1.1.1|224.0.0.2|VLAN20|VRF_BLUE| Dropping packet as max number of mroute or
nexthop is reached

2022-02-18T09:28:40.275256+00:00 8320 hpe-repld[2678]: MCAST_ANOMALY|-|DATA-PATH|-
|-|-|-|Could not allocate resources | linecard = e1937928-cccc-4027-a240-
aa54ba2de076 | err = Ingress resources exhausted

2022-02-18T09:28:40.283113+00:00 8320 ops-switchd[1214]: MCAST_ANOMALY|IPV4|DATA-
PATH|-|100.1.1.1|224.0.0.2|VLAN20|VRF_BLUE|Unable to add IPMC entry
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast boundary interface

show ip multicast boundary interface <interface-name>

Description

Displays IP Multicast boundary ACL configurations and packet drop counters for the specified interface.

Examples

The following example displays IP multicast boundary information for interface **1/1/1**.

```
switch# show ip multicast boundary interface vlan50
IP Multicast Boundary Configurations
-----
access-list ip permitssm
  20 permit any any 225.0.0.0/255.0.0.0
  30 permit any any 230.0.0.0/255.0.0.0
  40 permit any any 232.0.0.0/255.0.0.0

IP Multicast Boundary Rx packet drop counters
-----
PIM Joins/Prunes          0
PIM BSM                   0
PIM C-RP Advertisements   0
PIM Asserts               0
Multicast Data Packets     0
IGMP Joins                 0
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command Introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Users having admin privileges.

show ip pim

show ip pim [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows PIM router information on all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

- Multicast NSF is not supported for PIM RP enabled switches, therefore some transient traffic loss is expected during ISSU on RP routers where both PIM and MSDP are enabled.
- When PIM NSF status is inactive, the PIM NSF Time Remaining information is not shown.

Example

Showing IP PIM router information:

```
switch# show ip pim

PIM Global Parameters

VRF                               : default
PIM Status                       : Enabled
PIM SSM Status                   : Enabled
PIM SSM Range ACL                 : pim_ssm_grp_range_acl
Join/Prune Interval (sec)        : 60
SPT Threshold                    : Enabled
State Refresh Interval (sec)     : 60
PIM NSF Status                   : Active
PIM NSF Time Remaining (HH:MM:SS) : 00:01:21
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Added NSF information: PIM NSF status, PIM NSF Time Remaining
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rpf

show ip pim rpf [<source-ip-address> [<group-ip-address>]] [vrf <vrf-name> | all-vrfs]

Description

Shows PIM RPF details for the specified source or RP address in the given VRF. It shows the nexthop and interface through which shortest path to the source is available. Additionally, it prints if PIM neighborship is present on the nexthop. If VRF is not given, it displays for default VRF.

Parameter	Description
<IP-ADDR>	Show PIM RPF details for the given IPv4/IPv6 (X:X::X:X) address
vrfs	Shows PIM RPF information for specific VRF.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
all-vrfs	Shows PIM RPF details in all VRFs.

Examples

Showing PIM RPF for an IP address:

```
switch# [show ip pim rpf 1.1.1.1]

VRF: default
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask  Origin
In Use
-----
1.1.1.1         vlan10         10.1.1.1       yes              1.1.1.1/32      O
yes
```

Showing PIM RPF for all VRFs:

```
switch# [show ip pim rpf all-vrfs]

VRF: default
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask  Origin
In Use
-----
1.1.1.1         vlan10         10.1.1.1       yes              1.1.1.1/32      O
yes
10.1.1.1        vlan10         -               no               10.1.1.0/24      C
yes
10.1.1.2        vlan10         -               no               10.1.1.2/32      C
yes

VRF: red
IP Address      RPF Interface  RPF Nexthop    PIM Neighbor    RPF Route/Mask  Origin
In Use
-----
2.2.2.2         vlan20         20.0.0.1       yes              2.2.2.2/32      SU
yes
20.0.0.1        vlan20         -               no               20.0.0.0/24      C
```

```
yes
20.0.0.2      vlan20      -      no      20.0.0.2/32      C
yes
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim bsr

```
show ip pim bsr [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about BSR candidates in the domain and multicast groups it supports. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows PIM candidate BSR information for all VRFs.
vrf <VRF-NAME>	Optional. Shows PIM candidate BSR information for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing information about BSR candidates:

```
switch# show ip pim bsr all-vrfs
```


Status and Counters- PIM-SM Bootstrap Router Information

```
VRF                                     : default
E-BSR Address                         : 10.0.0.1
E-BSR Priority                         : 0
E-BSR Hash Mask Length                : 30
E-BSR Up Time                         : 3000 secs
Next Bootstrap Message                : 80 secs

C-BSR Admin Status                    : This system is a Candidate-BSR
C-BSR Address                         : 2.2.2.2/24
C-BSR Priority                         : 34
C-BSR Hash Mask Length                : 30
C-BSR Message Interval                : 76
C-BSR Source IP Interface             : vlan10

C-RP Admin Status                     : This system is a Candidate-RP
C-RP Address                         : 2.2.2.2
C-RP Hold Time                        : 150
C-RP Advertise Period                 : 60
C-RP Priority                         : 192
C-RP Source IP Interface              : vlan10

Group Address      Group Mask
-----
226.2.2.2          255.255.255.255
228.2.2.2          255.255.255.255
232.2.2.2          255.255.255.255

VRF                                     : green
E-BSR Address                         : 2.2.2.2
E-BSR Priority                         : 0
E-BSR Hash Mask Length                : 30
E-BSR Up Time                         : 3000 secs
Next Bootstrap Message                : 80 secs

C-BSR Admin Status                    : This system is a Candidate-BSR
C-BSR Address                         : 2.2.2.2/24
C-BSR Priority                         : 34
C-BSR Hash Mask Length                : 32
C-BSR Message Interval                : 60
C-BSR Source IP Interface             : vlan10

C-RP Admin Status                     : This system is a Candidate-RP
C-RP Address                         : 2.2.2.2
C-RP Hold Time                        : 150
C-RP Advertise Period                 : 60
C-RP Priority                         : 192
C-RP Source IP Interface              : vlan10

Group Address      Group Mask
-----
231.2.2.2          255.255.255.255
232.2.2.2          255.255.255.255
235.2.2.2          255.255.255.255
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim bsr elected

```
show ip pim bsr elected [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows information about the elected BSR in the domain and multicast groups it supports. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM elected bootstrap router information:

```
switch# show ip pim bsr elected all-vrfs

Status and Counters- PIM-SM Elected Bootstrap Router Information

VRF                               : default
E-BSR Address                     : 10.0.0.1
E-BSR Priority                     : 0
E-BSR Hash Mask Length            : 30
E-BSR Up Time                     : 3000 secs
Next Bootstrap Message            : 80 secs

VRF                               : green
E-BSR Address                     : 20.0.0.1
E-BSR Priority                     : 0
E-BSR Hash Mask Length            : 30
E-BSR Up Time                     : 3000 secs
Next Bootstrap Message            : 80 secs
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim bsr local

```
show ip pim bsr local [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about BSR candidates on the local router and multicast groups it supports. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing local Candidate BSR:

```
switch# show ip pim bsr local all-vrfs

Status and Counters - PIM-SM Local Candidate-BSR Information

VRF                               : default
C-BSR Admin Status                : This system is a Candidate-BSR
C-BSR Address                     : 2.2.2.2/24
C-BSR Priority                     : 34
C-BSR Hash Mask Length            : 30
C-BSR Message Interval            : 76
C-BSR Source IP Interface         : vlan10
```

```
VRF                                     : green
C-BSR Admin Status                     : This system is a Candidate-BSR
C-BSR Address                         : 2.2.2.2/24
C-BSR Priority                         : 34
C-BSR Hash Mask Length                : 32
C-BSR Message Interval                : 60
C-BSR Source IP Interface             : vlan10
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface

```
show ip pim interface [brief | all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
brief	Specifies brief interface information
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

The following example shows the information about PIM interfaces currently configured in the router for a HPE Aruba Networking 6200, 6300, 6400, 8100, 8325, 8360, 9300/9300S, and 10000 Switch series.

```
switch# show ip pim interface 1/1/2
```

PIM Interfaces

```
VRF: default
Interface: 1/1/2
Neighbor count: 2
IP Address: 50.1.1.4/24
Mode: bidir
Designated Router: NA
Proxy DF: false
Hello Interval (sec): 30
Hello Delay (sec): 5
Override Interval (msec): 2500      Lan Prune Delay: Yes
Propagation Delay (msec): 500        Configured DR Priority: NA
Operational DR Priority : NA
Neighbor Timeout: 105
```

Showing the PIM interface information in brief for the default VRF:

```
switch(config)# show ip pim interface brief
```

```
-----
--
VRF : default                                Total number of interfaces : 4
-----
--
Interface      IP Address      DR Address      Neighbor      Mode      VSX
              count
Role
-----
1/1/1          40.0.0.4/24     Nil             1             bidir     NA
vlan10         50.1.1.1/24     Nil             0             bidir     NA
vlan20         60.0.0.4/24     Nil             1             bidir     NA
vlan30         30.10.10.2/24   Nil             2             bidir     NA
loopback1      70.0.0.4/24     NA              NA             bidir     NA
-----
--
```

Showing PIM interface brief information for all VRFs:

```
switch(config)# show ip pim interface brief all-vrfs
```

```
-----
--
VRF : default                                Total number of interfaces : 1
-----
--
Interface      IP Address      DR Address      Neighbor      Mode      VSX
              count
Role
-----
```

```

--
1/3/1          31.1.1.1/30          Nil          0          sparse          N/A
-----
--
-----
--
VRF : vrf1          Total number of interfaces : 1
-----
--
1/3/2          32.1.1.1/30          Nil          0          sparse          N/A
-----
--

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Added support for BIDIR PIM on the 6200, 6300, 6400, 8100, 8325, 8360, 9300/9300S, 10000 Switch series
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name

show ip pim interface {<INTERFACE-NAME> [vsx-peer] | lag | loopback | tunnel | vlan <VLAN-ID> | vxlan} [vrf <VRF-NAME>]

Description

Shows detailed information about the PIM interface currently configured.

Parameter	Description
<INTERFACE-NAME>	Specifies an interface for showing PIM interface information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Parameter	Description
LAG	Shows LAG interface information.
loopback	Shows loopback interface information.
tunnel	Shows tunnel interface information.
vlan <VLAN-ID>	Specifies an interface for showing PIM interface information.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vxlan	Shows the VXLAN interface information.

Example

Showing PIM interface information for interface 1/1/2:

```
switch# show ip pim interface 1/1/2

PIM Interfaces

VRF: default

Interface   : 1/1/2
IP Address  : 50.0.0.4/24
Mode        : sparse

Designated Router :
Hello Interval (sec) : 30
Hello Delay (sec)   : 5

Override Interval (msec) : 2500      Lan Prune Delay : Yes
Propagation Delay (msec) : 500       DR Priority       : 1
Neighbor Timeout      : 105
```

Showing the PIM interface information for VLAN 10:

```
switch# show ip pim interface vlan 10

PIM Interfaces

VRF: red

Interface      : vlan10
Neighbor count : 1
IP Address     : 100.100.1.1/24
Mode           : sparse

Designated Router : 100.100.1.1
Proxy DR          : false
Hello Interval (sec) : 30
Hello Delay (sec)   : 5

Override Interval (msec) : 2500      Lan Prune Delay : Yes
Propagation Delay (msec) : 500       DR Priority       : 1
Neighbor Timeout      : 83
```

Showing the PIM interface information for VLAN 10 when anycast neighbors are present:

```

switch# show ip pim interface vlan 10

PIM Interfaces

VRF: red

Interface      : vlan10
Neighbor count : 1
IP Address     : 100.100.1.1/24
Mode           : sparse

Designated Router      : 100.100.1.1
Proxy DR               : false
Hello Interval (sec)   : 30
Hello Delay (sec)      : 5

Override Interval (msec) : 2500      Lan Prune Delay : Yes
Propagation Delay (msec) : 500       DR Priority      : 1
Neighbor Timeout       : 83

Anycast Neighbors Present : True
DR State                  : Non-DR
Operational DR Priority    : 30529026
Elected DR priority       : 50529027

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name counters

show ip pim interface <INTERFACE-NAME> counters [vsx-peer]

Description

Shows the PIM packet counters information for the specified interface.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to show packet counter information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not

Parameter	Description
	have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Example

Showing PIM packet counters for interface 1/1/5:

```
Switch(config)# show ip pim interface 1/1/5 counters
```

```
Interface   : 1/1/5
VRF         : default
```

Tx Counters :

Hello	310
State Refresh	0
Join/Prune	141
SSM Join/Prune	141
RP Advertisement	0
Graft	0
Graft Ack	0
Assert	0
Bsm	0
Register	0
Register Stop	0
SSM Register Stop	0

Rx Counters :

Hello	308
State Refresh	0
Join/Prune	0
SSM Join/Prune	0
RP Advertisement	0
Graft	0
Graft Ack	0
Assert	0
Bsm	0
Register	0
SSM Register	0
Register Stop	0
Register Drops(Register ACL hitcount)	0
Join/Prune Drops(RP ACL hitcount)	0

Rx Drop Counters :

Hello	0
State Refresh	0
Join/Prune	0
RP Advertisement	0

```
Graft                                0
Graft Ack                           0
Assert                              0
Bsm                                  0
Switch(config)#
```

Showing PIM packet counters for interface VLAN 1:

```
switch# show ip pim interface vlan1 counters
```

```
Interface      : vlan1
VRF            : default
```

Rx Counters :

```
Hello                                4
State Refresh                        0
Join/Prune                           1
RPadv                                0
Graft                                0
GraftAck                             0
Assert                              0
Bsm                                  0
Register                             0
Register Stop                         0
Register Drops(Register ACL hitcount) 10
Join/Prune Drops(RP ACL hitcount)     5
```

Tx Counters :

```
Hello                                9
State Refresh                        0
Join/Prune                           0
RPadv                                0
Graft                                0
GraftAck                             0
Assert                              0
Bsm                                  0
Register                             0
Register Stop                         0
```

Invalid Rx Counters :

```
Hello                                0
State Refresh                        0
Join/Prune                           0
RPadv                                0
Graft                                0
GraftAck                             0
Assert                              0
Bsm                                  0
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp

```
show ip pim rp [<group-ip>] [{vrf <vrf-name>}|all-vrfs]
```

Description

Displays the rendezvous point (RP) address for a particular group in the given VRF. The output of this command also includes the type of RP (static or dynamic) and the uptime for the mapping. This information can help verify that Group-to-RP mapping is consistent across all routers in the network. If the **group-ip** parameter is not included, the output of this command displays the group-to-RP mappings of those groups with active multicast traffic in the given VRF. If a VRF name is not specified, the output of this command displays information for the default VRF.

Parameter	Description
<group-ip>	Display group-to-RP mappings for the specified group.
vrf <VRF-NAME>	Specifies the name of a VRF. The default VRF is named default .
all-vrfs	Selects all VRFs.

Example

Showing RP mapping information for a single group:

```
switch# show ip pim rp 239.1.1.1

VRF: default

PIM-SM Group-to-Resultant_RP Mapping Information
Group Address   RP Address   RP Type   Up Time(HH:MM:SS)
-----
239.1.1.1      20.1.1.1    bsr       12:01:20
```

Showing RP mapping for all VRFs:

```
switch# show ip pim rp all-vrfs
VRF: default

PIM-SM Group-to-Resultant_RP Mapping Information
Group Address   RP Address   RP Type   Up Time(HH:MM:SS)
```

```

-----
239.1.1.1      20.1.1.1      bsr      15:10:45
239.1.1.2      40.1.1.1      static   05:07:30
239.1.1.3      Not Found     -        -

VRF: red

PIM-SM Group-to-Resultant_RP Mapping Information
Group Address  RP Address    RP Type      Up Time(HH:MM:SS)
-----
225.1.1.1      100.1.1.5     bsr          15:11:50

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-registered-source

`show ip pim rp-registered-sources <group-address> [source-address] [all-vrfs | vrf <vrf-name>]`

Description

Displays the registered sources information on the RP router. This command shows information about the active multicast flows that are registered by the source designated router (DR) to this Rendezvous Point (RP). When the multicast source becomes inactive, the entry will be removed from this table. Note that this command displays only the set of flows that have been registered successfully for which the current router is the RP.

Parameter	Description
<group-address>	Shows registered sources information for the group address. Format: x.x.x.x
<source-address>	(Optional) Shows registered sources information for the group from this source. Format: x.x.x.x Display registered sources information for group address.
vrf <VRF-NAME>	Displays registered sources information for a specific VRF.
all-vrfs	Displays registered sources information for all VRFs.

Example

The following example shows the registered sources information for all VRFs.

```
switch# show ip pim rp-registered-sources all-vrfs
Multicast flows registered with this RP
VRF : default
Total number of entries : 2
Source Address      Group Address      RP Address
-----
20.1.1.1            225.1.1.4          2.2.2.2
20.1.1.1            225.1.1.5          2.2.2.2

Multicast flows registered with this RP
VRF : red
Total number of entries : 2
Source Address      Group Address      RP Address
-----
30.1.1.1            229.1.1.1          4.4.4.4
30.1.1.1            229.1.1.2          4.4.4.4
```

The following example shows the registered sources information for a specific group and source address.

```
switch# show ip pim rp-registered-sources 229.1.1.10 30.1.1.1

Multicast flows registered with this RP
VRF : default
Total number of entries : 1
Source Address      Group Address      RP Address
-----
30.1.1.1            229.1.1.10        4.4.4.4

PIM-SM Group-to-Resultant_RP Mapping Information
Group Address  RP Address  RP Type  Up Time(HH:MM:SS)
-----
225.1.1.1      100.1.1.5   bsr      15:11:50
Showing RP mapping information for a single group:
```

```
Multicast flows registered with this RP
VRF : default
Total number of entries : 2
Source Address      Group Address      RP Address
-----
20.1.1.1            225.1.1.4          2.2.2.2
20.1.1.1            225.1.1.5          2.2.2.2

Multicast flows registered with this RP
VRF : red
Total number of entries : 2
Source Address      Group Address      RP Address
-----
30.1.1.1            229.1.1.1          4.4.4.4
30.1.1.1            229.1.1.2          4.4.4.4
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim neighbor

`show ip pim neighbor [<IP-ADDRESS>] [brief | all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<IP-ADDRESS>	Specifies an IP address.
brief	Specifies PIM neighbor information display in brief format.
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM neighbor information for the 5420, 6200, 6300, 6400, 8100, 8325, 8360, 9300/9300S, 10000 Switch series:

```
switch# show ip pim neighbor

PIM Neighbor

VRF                               : default
Total number of neighbors : 1

IP Address                       : 30.1.1.3
Interface                       : vlan30
Up Time (HH:MM:SS)              : 03:55:40
Expire Time (HH:MM:SS)          : 00:01:23
DR Priority                      : NA
Hold Time (HH:MM:SS)            : 00:01:45
Bidir Capable                   : True
```

Showing PIM neighbor information in brief for the default VRF:

```
switch# show ip pim neighbor brief
-----
-
VRF: default                               Total number of neighbor : 2
-----
-
Interface  Neighbor  Uptime    Expires    DR        Hold Time  Secondary
Address    (IPv4)    (HH:MM:SS) (HH:MM:SS) Priority    (HH:MM:SS) (IPv4)
-----
-
29091/1/1  40.0.0.5  11:54:21  00:01:31   NA        00:01:45   Nil
29101/1/2  50.0.0.5  00:03:23  00:01:23   NA        00:01:45
60.0.0.4,70.0.0.4-----
-----
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.13	Added support for BIDIR PIM on the 6200, 6300, 6400,8100, 8325, 8360, 9300, 10000 Switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim pending

```
show ip pim pending [<GROUP-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the pending joins on a PIM router. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Use this command to determine what flows are being requested on the PIM network. If data availability for a flow is expected, and a join for the flow is pending, the troubleshooting search moves to the source of that flow, since the routers are verified to be seeing the request for data.

Parameter	Description
<GROUP-ADDR>	Specifies a group address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing pending PIM joins:

```
switch# show ip pim pending
Join Pending
VRF : default
  Group 234.0.20.4
    (*,G) Pending
    Incoming Interface: 1/1/32
  Group 234.0.20.5
    (*,G) Pending
    Incoming Interface: 1/2/32
  Group 234.0.20.6
    (*,G) Pending
    Incoming Interface: 1/1/32
  Group 234.0.20.7
    (*,G) Pending
    Incoming Interface: 1/1/2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-candidate

```
show ip pim rp-candidate [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the candidate RP operational and configuration information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>all-vrfs</code>	Selects all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP candidate:

```
switch# show ip pim rp-candidate all-vrfs

Status and Counters- PIM-SM Candidate-RP Information

VRF                               : Green
C-RP Admin Status                 : This system is a Candidate-RP
C-RP Address                      : 10.1.1.27
C-RP Hold Time                    : 150
C-RP Advertise Period             : 60
C-RP Priority                      : 192
C-RP Source IP Interface         : Vlan10

Group Address    Group Mask
-----
239.10.10.240    255.255.255.252
236.0.0.0        255.255.255.0

VRF                               : Red
C-RP Admin Status                 : This system is a Candidate-RP
C-RP Address                      : 20.1.1.27
C-RP Hold Time                    : 150
C-RP Advertise Period             : 60
C-RP Priority                      : 192
C-RP Source IP Interface         : Vlan20

Group Address    Group Mask
-----
239.10.10.240    255.255.255.252
236.0.0.0        255.255.255.0
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-set

```
show ip pim rp-set [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for both the learned C-RP assignments and any statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set information:

```
switch# show ip pim rp-set all-vrfs

VRF: default

Status and Counters - PIM-SM Static RP-Set Information
Group Address      Group Mask          RP Address          Override
-----
233.100.128.255    255.255.255.255    100.10.10.1        Yes
238.100.128.255    255.255.255.255    100.10.10.3        Yes

Status and Counters - PIM-SM Learned RP-Set Information
Group Address      Group Mask          RP Address          Hold Time  Expire Time
-----
223.2.2.34         255.0.0.0          9.0.0.25           12         0

VRF: green

Status and Counters - PIM-SM Static RP-Set Information
Group Address      Group Mask          RP Address          Override
-----
226.102.128.255    255.255.255.255    105.10.10.3        Yes
234.102.128.255    255.255.255.255    110.10.10.3        Yes

Status and Counters - PIM-SM Learned RP-Set Information
Group Address      Group Mask          RP Address          Hold Time  Expire Time
-----
223.2.2.34         255.0.0.0          9.0.0.25           12         0
```

229.2.2.34	255.0.0.0	9.0.0.25	10	0



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-set learned

show ip pim rp-set learned [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows the multicast group support for dynamically learned RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set learned information:

```
switch# show ip pim rp-set learned all-vrfs

VRF: default

Status and Counters - PIM-SM Learned RP-Set Information
Group Address      Group Mask      RP Address      Hold Time      Expire Time
-----
223.2.2.34         255.0.0.0       9.0.0.25        12             0

VRF: green
```

```
Status and Counters - PIM-SM Learned RP-Set Information
Group Address      Group Mask      RP Address      Hold Time      Expire Time
-----
223.2.2.34         255.0.0.0       9.0.0.25        12             0
229.2.2.34         255.0.0.0       9.0.0.25        10             0
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-set static

```
show ip pim rp-set static [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Selects all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM Static RP set information:

```
switch# show ip pim rp-set static all-vrfs

VRF: default

Status and Counters - PIM-SM Static RP-Set Information
```

Group Address	Group Mask	RP Address	Override
233.100.128.255	255.255.255.255	100.10.10.1	Yes
238.100.128.255	255.255.255.255	100.10.10.3	Yes

VRF: green

Status and Counters - PIM-SM Static RP-Set Information

Group Address	Group Mask	RP Address	Override
226.102.128.255	255.255.255.255	105.10.10.3	Yes
234.102.128.255	255.255.255.255	110.10.10.3	Yes



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rpf-override

show ip pim rpf-override [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows the RPF override configuration, which can be useful information when troubleshooting potential RPF misconfigurations. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF

Parameter	Description
all-vrfs	Optional. Shows PIM RPF override information for all VRFs.
vrf <VRF-NAME>	Optional. Shows PIM RPF override information for a particular VRF. If the <VRF-NAME> is not specified, it shows information for the default VRF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RPF override:

```
switch# show ip pim rpf-override all-vrfs

VRF          : default
Static RPF Override
Multicast Source RPF IP Address
-----
10.0.0.2/32   1.1.1.1

VRF          : green
Static RPF Override
Multicast Source RPF IP Address
-----
10.0.0.2/32   1.1.1.1
10.1.1.1/32   1.1.1.2
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-registered-source

show ip pim rp-registered-sources <group-address> [source-address] [all-vrfs | vrf <vrf-name>]

Description

Displays the registered sources information on the RP router. This command shows information about the active multicast flows that are registered by the source designated router (DR) to this Rendezvous Point (RP). When the multicast source becomes inactive, the entry will be removed from this table. Note that this command displays only the set of flows that have been registered successfully for which the current router is the RP.

Parameter	Description
<group-address>	Shows registered sources information for the group address. Format: x.x.x.x
<source-address>	(Optional) Shows registered sources information for the group from this source. Format: x.x.x.x

Parameter	Description
	Display registered sources information for group address.
vrf <VRF-NAME>	Displays registered sources information for a specific VRF.
all-vrfs	Displays registered sources information for all VRFs.

Example

The following example the registered sources information for all VRFs.

```
switch# show ip pim rp-registered-sources all-vrfs
Multicast flows registered with this RP
VRF : default
Total number of entries : 2
Source Address      Group Address      RP Address
-----
20.1.1.1            225.1.1.4          2.2.2.2
20.1.1.1            225.1.1.5          2.2.2.2

Multicast flows registered with this RP
VRF : red
Total number of entries : 2
Source Address      Group Address      RP Address
-----
30.1.1.1            229.1.1.1          4.4.4.4
30.1.1.1            229.1.1.2          4.4.4.4
```

The following example the registered sources information for a specific group and source address.

```
switch# show ip pim rp-registered-sources 229.1.1.10 30.1.1.1

Multicast flows registered with this RP
VRF : default
Total number of entries : 1
Source Address      Group Address      RP Address
-----
30.1.1.1            229.1.1.10        4.4.4.4

PIM-SM Group-to-Resultant_RP Mapping Information
Group Address  RP Address  RP Type  Up Time(HH:MM:SS)
-----
225.1.1.1      100.1.1.5   bsr      15:11:50
Showing RP mapping information for a single group:
```

```
Multicast flows registered with this RP
VRF : default
Total number of entries : 2
Source Address      Group Address      RP Address
-----
20.1.1.1            225.1.1.4          2.2.2.2
20.1.1.1            225.1.1.5          2.2.2.2

Multicast flows registered with this RP
VRF : red
Total number of entries : 2
```

Source Address	Group Address	RP Address
-----	-----	-----
30.1.1.1	229.1.1.1	44.4.4
30.1.1.1	229.1.1.2	4.4.4.4



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rpf-override source

`show ip pim rpf-override source <IP-ADDR> [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the RPF override configuration for the specified source. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>source <IP-ADDR></code>	Specifies the RPF source address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<code>all-vrfs</code>	Selects all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing PIM RPF override source:

```
switch# show ip pim rpf-override source 10.0.0.2

VRF                : default
Static RPF Override
```



```
Multicast Source RPF IP Address
-----
10.0.0.2          1.1.1.1
```

Showing PIM RPF override source for all VRFs:

```
switch# show ip pim rpf-override source 10.0.0.2 all-vrfs

VRF          : default
Static RPF Override
Multicast Source RPF IP Address
-----
10.0.0.2          1.1.1.1

VRF          : green
Static RPF Override
Multicast Source RPF IP Address
-----
10.0.0.2          1.1.1.1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim tree-state

```
show ip pim tree-state {<group-ip> [<source-ip>]}|brief [{vrf <vrf-name>}] all-vrfs]
```

Description

Displays upstream join states for a specified group and source address in a VRF.

The command displays upstream state, upstream interface and RPF neighbor used to send join messages and a list of downstream interfaces from which join messages are received.

The set of downstream interfaces in this command may not show the final list of outgoing interfaces for a flow, which is computed from various internal states and is shown in the output of the command [show ip mroute](#).

Parameter	Description
<group-ip>	Shows PIM Join details for the specified group IP address
<source-ip>	Shows PIM Join details for the specified source IP address. If a source address is not specified, only *,G states are displayed for the specified group. If a source address is specified, (S,G) states are displayed along with (*,G) states and (S,G,RPT) states wherever applicable.
brief	Display brief details for the multicast group and source in a table format.
vrf <VRF-NAME>	Show join state details for the specified VRF.
all-vrfs	Show join state details for all VRFs.

Usage

The output of this command can indicate one of the following two multicast group (*,G) and multicast source and group (S,G) upstream states:

- **Joined** : Join sent to upstream RPF neighbor.
- **Not Joined** : Joins not sent upstream.

The following states are applicable to the multicast group (*,G), and root path tree (S,G,RPT) only:

- **Pruned** : Traffic from the source is arriving on the shortest path tree, (*,G) Joined, but (S,G,RPT) pruned.
- **Not Pruned** : Traffic from the multicast group (*,G) Joined, and (S,G,rpt) not pruned.
- **RPT Not Joined** : The multicast group (*,G) has not joined.

Examples

Display multicast group (*,G) join information for the VRF **red**.

```
show ip pim tree-state 239.1.1.1 vrf red
(*,G) Information for Group 239.1.1.1
VRF: red
Upstream Information:
State                : Joined
Joined Interface     : vlan50
RPF Neighbor         : 20.1.1.2
Uptime               : 01:58:30
Downstream Information:
Interfaces            : vlan50, vlan201
```

Display group (*,G), source and group (S,G), and root-path tree (S,G, RPT) Information for group **239.1.1.1** and source IP **30.1.1.1**.

```
show ip pim tree-state 239.1.1.1 30.1.1.1 vrf red
(*,G) Information for Group 239.1.1.1
VRF: red
```

```

Upstream Information:
State                  : Joined
Joined Interface      : vlan50
RPF Neighbor         : 20.1.1.2
Uptime               : 01:58:30
Downstream Information:
Interfaces            : vlan200
(S,G) Information for Group 239.1.1.1 Source 30.1.1.1
Upstream Information:
State                  : Joined
Joined Interface      : vlan30
RPF Neighbor         : 40.1.1.2
Uptime               : 01:57:30
SPT bit set          : True
Downstream Information:
Interfaces            : vlan200
(S,G,RPT) Information for Group 239.1.1.1 Source 30.1.1.1
Upstream Information:
State                  : Pruned
Joined Interface      : vlan50
RPF Neighbor         : 20.1.1.2
Uptime               : 01:58:30
Downstream Information:
Interfaces            : vlan200

```

Display brief information for the IP PIM tree state.

```

switch# show ip pim tree-state brief
State abbreviations :
J - Joined  NJ - Not Joined  RPTNJ - RPT Not Joined
P - Pruned  NP - Not Pruned
-----
VRF : default
-----
Group Address      Source Address      RPF      Uptime      State  Type
Neighbor          (HH:MM:SS)
-----
239.1.1.1          *                   10.1.1.2  01:58:30    J      *,G
239.1.1.1          40.0.0.6           10.1.1.2  01:58:30    J      S,G
239.1.1.2          *                   10.1.1.2  01:58:30    J      *,G
239.1.1.2          40.0.0.6           20.1.1.2  01:58:30    J      S,G
239.1.1.2          40.0.0.6           10.1.1.2  01:58:30    P      S,G,RPT
-----

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.14	Command Introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

sources-per-group

```
sources-per-group <limit>
no sources-per-group <limit>
```

Description

Configures the total number of sources allowed for a group on the router. By default, there is no limit on the number of sources for a group. When the number of sources for a group exceeds the configured limit, multicast traffic from additional sources will be dropped.

The **no** form of this command removes the currently configured limit value.

Parameter	Description
<limit>	Specifies the value to be configured as the sources allowed per group. Range: 1 to 4294967295.

Usage

Flows exceeding the limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration does not allow new sources for the group. At the time of configuration, if the device has more sources for the given group than the configured value, already allowed sources continue to exist until they are removed.

The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage.

Examples

Configuring and removing the sources allowed per group:

```
switch(config)# router pim
switch(config-pim)# sources-per-group 4
switch(config-pim)# no sources-per-group
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

spt-threshold

```
spt-threshold
no spt-threshold
```

Description

Enables the router to switch the multicast traffic flows to the shortest path tree. Default is enabled. The **no** form of this command disables the routers ability to switch the multicast traffic flows to the shortest path tree.

To apply this configuration a user needs to apply disable/enable PIM globally.

Example

Enabling and disabling the SPT threshold:

```
switch(config)# router pim
switch(config-pim)# spt-threshold
switch(config-pim)# no spt-threshold
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

accept-register access-list

```
accept-register access-list <ACL-RULE>
no accept-register access-list <ACL-RULE>
```

Description

Configures ACL on RP to filter PIM Register packets from unauthorized sources. The ACL specified will contain the (S,G) traffic in register packets to permitted or denied.

The **no** form of this command removes the currently configured ACL rule.

Parameter	Description
<ACL-RULE>	Specifies the ACL rule name.

Usage

When register ACL is associated with a PIM Router, PIM protocol will store the source and destination address details along with the action (permit or deny).

Upon receiving the register messages, a look up is made to check if the S and G in the packet is in the permitted list. If there is no match or if there is a deny rule match, a register stop message is immediately sent and the packet is dropped and no further action is taken. Permitted packets will go through the normal flow.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Examples

Configuring ACL on RP with an ACL rule named **pim_regv6_acl**:

```
switch(config)# access-list ipv6 pim_regv6_acl
switch(config-acl-ipv6)# 10 permit any 20:::1 ff1e::1
switch(config-acl-ipv6)# 20 deny any 30:::1 ff1e::3
switch(config)# router pim6
switch(config-pim6)# accept-register access-list pim_regv6_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

accept-rp

```
accept-rp <IPv6-ADDR> access-list <ACL-RULE>
no accept-rp <IPv6-ADDR> access-list <ACL-RULE>
```

Description

Enables PIM router to filter PIM join/prune messages destined for a specific RP and specific groups. The ACL specifies the group addresses which are allowed or denied. Up to 8 RP addresses and group ACL can be associated with the PIM router.

The **no** form of this command removes the currently configured ACL rule.

Parameter	Description
<IPv6-ADDR>	Specifies an address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<ACL-RULE>	Specifies the ACL rule name.

Usage

PIM will store the accepted RP address and the associated group ACL. When a join or prune message is received, a RP look up is made for the packet. If the RP is in the configured list and if the group in the join/prune packet is allowed in the ACL, the packet is allowed. Otherwise the packet is dropped.

To allow join/prune message from any groups, group address in the ACL can be wild-carded. In this case, only RP address check is performed.

This command impacts only (*,G) join/prune messages. If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.



If there is an active flow which is in the SPT, the traffic flow through the SPT will continue. Only (*,G) join/prune messages are dropped. (S,G) join/prune messages will not be impacted.

Examples

Configuring ACL on RP with an ACL rule named **pim_rpv6_grp_acl** to filter join/prune messages:

```
switch(config-pim)# access-list ip pim_rpv6_grp_acl
switch(config-acl-ipv6)# 10 permit any any ff2e::2/64
switch(config-acl-ipv6)# 20 permit any any ffe::1/64
switch(config-acl-ipv6)# router pim6
switch(config-pim6)# accept-rp 30::1 access-list pim_rpv6_grp_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

bsr-candidate bsm-interval

```
bsr-candidate bsm-interval <INTERVAL-VALUE>
no bsr-candidate bsm-interval
```

Description

Configures the interval in seconds to send periodic RP-Set messages to all PIM-SM interfaces on a router that operates as the BSR in a domain. This setting must be smaller than the **rp-candidate hold-time** settings (range of 30 to 255; default 150) configured in the RPs operating in the domain.

The **no** form of this command removes the currently configured value and sets it to the default of 60 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the BSR-candidate BSM interval in seconds. Range: 5 to 300. Default: 60.

Example

Configuring and removing BSR-candidate BSM-interval:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate bsm-interval 150
switch(config-pim6)# no bsr-candidate bsm-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

bsr-candidate hash-mask-length

```
bsr-candidate hash-mask-length <LENGTH-VALUE>
no bsr-candidate hash-mask-length
```

Description

Controls the distribution of multicast groups among the C-RP, in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) when allocating this distribution. A longer hash-mask-length results in fewer multicast groups, for each block of group addresses assigned to the RPs. Multiple blocks of addresses assigned to each C-RP results in wider dispersal of addresses. Includes enhanced load-sharing for the multicast traffic for the different groups that are used in the domain at the same time.

The **no** form of this command removes currently configured value and sets to the default of 126.

Parameter	Description
<LENGTH-VALUE>	Specifies the length (in bits) of the hash mask. Range: 1 to 128. Default: 126.

Example

Configuring and removing the BSR-candidate hash-mask-length:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate hash-mask-length 4
switch(config-pim6)# no bsr-candidate hash-mask-length
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

bsr-candidate priority

```
bsr-candidate priority <PRIORITY-VALUE>
no bsr-candidate priority
```

Description

Configures the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the BSR of the domain. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain.

The **no** form of this command removes currently configured value and sets to the default of 0.

Parameter	Description
<PRIORITY-VALUE>	Specifies the priority for the Candidate Bootstrap router. Range: 0 to 255. Default: 0.

Example

Configuring and removing the BSR-candidate priority:

```
switch(config) # router pim6
switch(config-pim6) # bsr-candidate priority 250
switch(config-pim6) # no bsr-candidate priority
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

bsr-candidate source-ip-interface

```
bsr-candidate source-ip-interface <INTERFACE-NAME>
no bsr-candidate source-ip-interface <INTERFACE-NAME>
```

Description

Configures the router to advertise itself as a candidate PIM-SM BSR on the interface specified, and enables BSR candidate operation. The result makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. One BSR candidate interface is allowed per-router.

The **no** form of this command removes the Candidate BSR configuration.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the interface to use as a source for Candidate-BSR router IP address. Interface can be a VLAN interface, routed interface, or LAG. PIM-SM must be enabled on this interface with the command ipv6 pimv6-sparse enable .

Example

Configuring and removing the BSR-candidate interface:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim6)# no rp-candidate source-ip-interface 1/1/4
```

Configuring and removing the BSR-candidate sub-interface:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim6)# no rp-candidate source-ip-interface 1/1/4
```

Configuring sub-interface 1/1/19/10 as Candidate BSR:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate source-ip-interface 1/1/19.10
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

disable

disable

Description

Disables PIMv6 globally on the router.



Using the **disable** command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables PIMv6 globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

ipv6 mroute

ipv6 mroute <SRC-ADDR/SRC-MASK> <RPF-ADDRESS> | <INTERFACE-NAME>

Description

Configures multicast reverse path (RPF) forwarding static routes. This command is an alias of the **rpf-override** command.

The **no** form of this command removes the mroute configuration.

Parameter	Description
<SRC-ADDR>	Specifies the multicast source address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<SRC-MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<RPF-ADDR>	Specifies the RPF address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<INTERFACE-NAME>	Specifies the RPF interface name.

Usage

Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.

RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified. The RPF-address indicates one of two distinct RPF candidates:

1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of **<source-addr/src-mask>**.

2. A local router address on a PIM-enabled interface to which **<source-addr/src-mask>** is directly connected. If configured, the local router will assume the role of DR for this flow and registers the flow with an RP.

Example

Configuring and removing IP mroute:

```
switch(config-pim)# router pim6
switch(config-pim6)# ipv6 mroute 50::4/24 tunnel1
switch(config-pim6)# no ipv6 mroute 50::4/24 tunnel1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 pim6-sparse

```
ipv6 pim6-sparse {enable | disable}
no ipv6 pim6-sparse [enable]
```

Description

Enables or disables PIM-SM on the current interface. PIM-SM is disabled by default on an interface. An IPv6 address must be configured on the interface to enable PIM-SM.

Parameter	Description
enable	Enables PIM-SM on the interface. IPv6 address must be configured on the interface to enable PIM-SM (use the ipv6 address <X:X::X:X/M> command).
disable	Disables PIM SM on the interface.

Examples

Enabling and disabling PIM-SM on an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 2001::01/64
switch(config-if-vlan)# ipv6 pim6-sparse enable
switch(config-if-vlan)# ipv6 pim6-sparse disable
```

Enabling and disabling PIM-SM on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 address 90::1/64
switch(config-subif)# ipv6 pim6-sparse enable
switch(config-subif)# ipv6 pim6-sparse disable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse bfd

```
ipv6 pim6-sparse bfd [disable]
no ipv6 pim6-sparse bfd
```

Description

Configures BFD on a per-interface basis for an interface associated with the PIM process.

The **no** form of this command removes the BFD configuration on the interface and sets it to the default configuration.



If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the **ipv6 pim6-sparse bfd disable** command.

If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the **ipv6 pim6-sparse bfd** command.

Parameter	Description
disable	Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan 40  
switch(config-if-vlan)# ipv6 pim6-sparse bfd
```

Disabling the BFD configuration on the interface:

```
switch(config-if-vlan)# ipv6 pim6-sparse bfd disable
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ipv6 pim6-sparse bfd
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse dr-priority

```
ipv6 pim6-sparse dr-priority <PRIORITY-VALUE>  
no ipv6 pim6-sparse dr-priority
```

Description

Changes the router priority for the designated router (DR) election process in the current interface. A numerically higher value means a higher priority. If multiple routes share the highest priority, the router with the highest IP address is selected as the DR.

The **no** form of this command removes currently configured value and sets to the default of 1.

Parameter	Description
<PRIORITY-VALUE>	Specifies the priority value to use on the interface in the DR election process. Range: 0 to 4294967295. Default: 1.

Examples

Configuring and removing the interface priority value:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse dr-priority 4444
switch(config-if-vlan)# no ipv6 pim6-sparse dr-priority
```

Configuring and removing the interface priority value:

```
switch(config)# interface 1/1/19.10
switch(config-if-vlan)# ipv6 pim6-sparse dr-priority 2000
switch(config-if-vlan)# no ipv6 pim6-sparse dr-priority
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse hello-delay

```
ipv6 pim6-sparse hello-delay <DELAY-VALUE>
no ipv6 pim6-sparse hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The **no** form of this command removes currently configured value and sets to the default of 5 seconds.

Parameter	Description
<DELAY-VALUE>	Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Range: 0 to 5. Default: 5.

Usage

- In cases where a new interface activates connections with multiple routers. If all the connected routers sent hello packets at the same time, the receiving router could become momentarily

overloaded.

- This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse hello-delay 4
switch(config-if-vlan)# no ipv6 pim6-sparse hello-delay
```

Configuring and removing hello-delay on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse hello-delay 4
switch(config-subif)# no ipv6 pim6-sparse hello-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse hello-interval

```
ipv6 pim6-sparse hello-interval <INTERVAL-VALUE>
no ipv6 pim6-sparse hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface. The **no** form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the frequency at which PIM Hello messages are transmitted on this interface in seconds. Range: 5 to 300. Default: 30.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing sparse hello-interval:

```
switch(config-if) # ipv6 pim6-sparse hello-interval 60
switch(config-if) # no ipv6 pim6-sparse hello-interval
```

Configuring and removing sparse hello-interval on a sub-interface:

```
switch) config) # interface 1/1/19.10
switch(config-subif) # ipv6 pim6-sparse hello-interval 100
switch(config-subif) # no ipv6 pim6-sparse hello-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse ipv6-addr

ipv6 pim6-sparse ipv6-addr {<IPv6-ADDR-VALUE> | any}

```
no ipv6 pim6-sparse ipv6-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM-SM packets sent from the interface or to use the specific IPv6 address.

The **no** form of this command removes the currently configured value and sets to the default of **any**.

Parameter	Description
<code><IP-ADDR-VALUE></code>	Specifies the source IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<code>any</code>	Specifies dynamically determining the source IP from the current IP address of the interface.

Examples

Configuring and removing source IP address:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse ipv6-addr 2001::02
switch(config-if-vlan)# no ipv6 pim6-sparse ipv6-addr
```

Configuring and removing source IP address on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse ipv6-addr 2001:1::1
switch(config-if-vlan)# no ipv6 pim6-sparse ipv6-addr 2001:1::1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse lan-prune-delay

```
ipv6 pim6-sparse lan-prune-delay
no ipv6 pim6-sparse lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default is enabled.

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

The **no** form of this command disables the LAN prune delay option.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse lan-prune-delay
switch(config-if-vlan)# no ipv6 pim6-sparse lan-prune-delay
```

Enabling and disabling the LAN prune delay on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse lan-prune-delay
switch(config-subif)# no ipv6 pim6-sparse lan-prune-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse override-interval

```
ipv6 pim6-sparse override-interval <INTERVAL-VALUE>
no ipv6 pim6-sparse override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The **no** form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameter	Description
<code><INTERVAL-VALUE></code>	Specifies the override interval of a LAN Prune Delay option in ms. Range: 500 to 6000. Default: 2500.

Usage

A router sharing a VLAN with other multicast routers uses the override-interval value along with the propagation-delay value to compute the **lan-prune-delay** setting. The setting specifies how long to wait for a PIM-SM join after receiving a prune packet from downstream for a particular multicast group.

Example scenario:

A network may have multiple routers sharing VLAN X. When an upstream router is forwarding traffic from multicast group X to VLAN Y, if one of the routers on VLAN Y does not want this traffic, it issues a prune response to the upstream neighbor. The upstream neighbor then goes into a prune pending state for group X on VLAN Y. During this period, the upstream neighbor continues to forward the traffic. During the pending period, another router on VLAN Y can send a group X join to the upstream neighbor. If this happens, the upstream neighbor drops the prune pending status and continues forwarding the traffic. But if no routers on the VLAN send a join, the upstream router prunes.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse override-interval 4000
switch(config-if-vlan)# no ipv6 pim6-sparse override-interval
```

Configuring and removing the override interval on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse override-interval 5000
switch(config-subif)# no ipv6 pim6-sparse override-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
	config-lag-if config-subif	

ipv6 pim6-sparse propagation-delay

```
ipv6 pim6-sparse propagation-delay <DELAY-VALUE>
no ipv6 pim6-sparse propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The **no** form of this command removes currently configured value and sets to the default of 500 ms.

Parameter	Description
<DELAY-VALUE>	Specifies the propagation delay value in ms. Range: 250 to 2000. Default: 500.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse propagation-delay 400
switch(config-if-vlan)# no ipv6 pim6-sparse propagation-delay
```

Configuring and removing the propagation delay on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse propagation-delay 1000
switch(config-subif)# no ipv6 pim6-sparse propagation-delay
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

join-prune-interval

```
join-prune-interval <INTERVAL-VALUE>
no join-prune-interval
```

Description

Configures the frequency at which the router will send periodic join or prune-interval messages. The **no** form of this command sets the interval to the default value of 60 seconds.

Parameter	Description
<INTERVAL-VALUE>	Specifies the join-prune-interval in seconds. Range 5 to 65535. Default: 60.

Examples

Configuring join prune interval:

```
switch(config)# router pim6
switch(config-pim6)# join-prune-interval 400
switch(config-pim6)# no join-prune-interval
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

no ipv6 pim6-sparse

```
no ipv6 pim6-sparse
```

Description

Removes all the PIM-SM related IPv6 configurations for the interface.

Example

Removing PIM-SM configuration:


```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-sparse
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

rp-address access list

```
rp-address <IPv6-ADDR> [access-list <ACL-NAME>] [override]
no rp-address <IPv6-ADDR> [access-list <ACL-NAME>] [override]
```

Description

Statically configures the router as the RP and associates the static RP to the specified ACL.

The **no** form of this command removes static RP ACL configuration.

Parameter	Description
<i><IPv6-ADDR></i>	Specifies an address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<i>access-list <ACL-NAME></i>	Specifies the name of the access control list.
<i>override</i>	Specifies whether or not static RP configuration precedes the information learned by a BSR.

Usage

The ACL includes a list of permitted/ denied group addresses for the specified RP.

- When configured on a source DR, only permitted group addresses are registered to the RP. When applied on other routers, (*,G) PIM join/prune messages are filtered according to the applied ACL.
- Only destination group addresses in the ACEs are filtered and any other fields configured in the ACE are ignored. If only PIM (*,G) messages need to be filtered, configure **accept-rp** ACLs.

- When static RP ACL is configured, only one static RP can be configured per VRF and that configured RP handles all the multicast groups in range ff00::/8.



A change in the RP ACL does not impact the flows that have already switched to SPT. Only when the source information is expired and the RP is needed to establish the multicast tree, is the change in the ACL reflected. If the source is always active, PIM can be disabled and re-enabled to clear the learned sources information and re-establish multicast trees based on the latest RP ACL configurations.

Examples

Configuring the static RP ACL:

```
...
access-list ip static_rp6_acl
10 permit any any ff2e::2/64
20 permit any any ff1e::1/64

switch(config)# router pim6
switch(config-pim6)# rp-address 30::1 access-list static_rp6_acl
```

Removing the static RP ACL configuration:

```
switch(config-pim)# no rp-address 30::1 access-list static_rp6_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Added optional access list parameter [access-list <ACL-NAME>]
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-address

```
rp-address <IPv6-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
no rp-address <IPv6-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
```

Description

Statically configures the router as the RP for a specified multicast group or range of multicast groups. This must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv6 multicast addresses.

The **no** form of this command removes static RP configuration and its precedence.

Parameter	Description
<code><IPv6-ADDR></code>	Specifies an address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<code><GRP-ADDR></code>	Specifies the range of multicast group addresses in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<code><GRP-MASK></code>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<code>override</code>	Specifies higher precedence to static RP over Candidate RP.

Usage

Where a static RP and a C-RP are configured to support the same multicast groups and the multicast group mask for the static RP is equal to or greater than the same mask for the applicable C-RPs, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a backup RP for the configured group. Without `override`, the C-RP has precedence over a static RP configured for the same multicast group or groups.

Examples

```
switch(config)# router pim6
switch(config-pim6)# rp-address 2001::01 ff08::1:3/64 override
switch(config-pim6)# rp-address 2002::02 ff08::1:4/64
switch(config-pim6)# no rp-address 2002::02 ff08::1:4/64
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate group-prefix

```
rp-candidate group-prefix <GRP-ADDR/GRP-MASK>
no rp-candidate group-prefix <GRP-ADDR/GRP-MASK>
```

Description

Adds multicast group address to the current Candidate Rendezvous Point (C-RP) configuration. The **no** form of this command removes C-RP multicast group address.

Parameter	Description
<code><GRP-ADDR></code>	Specifies the multicast group address in IPv6 format (<code>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</code>), where x is a hexadecimal number from 0 to F.
<code><GRP-MASK></code>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

Configuring and removing candidate group prefix:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate group-prefix ff08::1:3/64
switch(config-pim6)# no rp-candidate group-prefix ff08::1:3/64
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

rp-candidate hold-time

```
rp-candidate hold-time <TIME-VALUE>
no rp-candidate hold-time
```

Description

Changes the hold-time a C-RP includes in its advertisements to the BSR.

Hold-time is included in the advertisements the C-RP periodically sends to the elected BSR for the domain. Also updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming it has become unavailable.

The **no** form of this command removes the currently configured value and sets it to the default value 150 seconds.

Parameter	Description
<code><TIME-VALUE></code>	Specifies the hold-time value in seconds to be sent in C-RP-Adv messages. Range: 30 - 255. Default: 150.

Example

Setting and removing the candidate holdtime:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate hold-time 250
switch(config-pim6)# no rp-candidate hold-time
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

rp-candidate priority

```
rp-candidate priority <PRIORITY-VALUE>
no rp-candidate priority
```

Description

Changes the current priority setting for a C-RP. Where multiple C-RP configurations are used to support the same multicast groups, the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority.

The **no** form of this command removes the currently configured value and sets it to the default of 192.

Parameter	Description
<code><PRIORITY-VALUE></code>	Specifies the priority value for the Candidate-RP router. Range: 0 to 255. Default: 192.

Example

Configuring and removing candidate priority:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate priority 250
switch(config-pim6)# no rp-candidate priority
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate source-ip-interface

```
rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
no rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
```

Description

Enables the Candidate Rendezvous Point (C-RP) operation, and configures the router to advertise itself as a C-RP to the Bootstrap Router (BSR) for the current domain.

This step includes the option to allow the C-RP to be a candidate for all possible multicast groups, or for up to four multicast groups, or ranges of groups. If group-prefix is not given, it considers for all multicast group addresses.

The **no** form of this command removes the C-RP configuration.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to use as a source for the C-RP router IP address.
group-prefix <GRP-ADDR/GRP-MASK>	Specifies the multicast group address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. And the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

Configuring a C-RP using VLAN 40 as the source for the C-RP router IP address and associating the ff08::1:3/64 multicast group with the C-RP router:

```
switch(config)# router pim6  
switch(config-pim6)# rp-candidate source-ip-interface vlan40 group-prefix  
ff08::1:3/64
```

Configuring a C-RP using loopback1 as the source for the C-RP router IP address and associating the ff08::1:3/64 multicast group with the C-RP router:

```
switch(config)# router pim6  
switch(config-pim6)# rp-candidate source-ip-interface loopback1 group-prefix  
ff08::1:3/64
```

Configuring sub-interface 1/1/19.10 as candidate RP:

```
switch(config)# router pim6  
switch(config-pim6)# rp-candidate source-ip-interface 1/1/19.10
```

Removing the candidate source IP interface:

```
switch(config-pim6)# no rp-candidate source-ip-interface vlan20
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

rpf-override

```
rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR| INTERFACE-NAME>  
no rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR| INTERFACE-NAME>
```

Description

The Reverse Path Forward (RPF) override, allows overriding the normal RPF lookup mechanism, and indicates to the router that it may accept multicast traffic on an interface other than the one that the RPF lookup mechanism would normally select. This includes accepting traffic from an invalid source IP address for the subnet or VLAN that is directly connected to the router. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.

The **no** form of this command removes currently configured RPF entry.

Parameter	Description
<SRC-ADDR>	Specifies the multicast source address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<SRC-MASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<RPF-ADDR>	Specifies the RPF address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<INTERFACE-NAME>	Specifies the RPF interface name.

Usage

Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.

RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified. The RPF-address indicates one of two distinct RPF candidates:

1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of **<source-addr/src-mask>**.
2. A local router address on a PIM-enabled interface to which **<source-addr/src-mask>** is directly connected. If configured, the local router will assume the role of DR for this flow and registers the flow with an RP.

Example

Configuring and removing RPF override:

```
switch(config)# router pim6
switch(config-pim6)# rpf-override 50::4/24 40::1
switch(config-pim)# no rpf-override 50::4/24 40::1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

show ipv6 mroute <GROUP-ADDR>

show ipv6 mroute <GROUP-ADDR> [<SOURCE-ADDR>] [all-vrfs | vrf <vrf-name>] [vsx-peer]

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<GROUP-ADDR>	Specifies a group address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<SOURCE-ADDR>	Specifies a source IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group ff08::1:3 and VRF green:

```
switch# show ipv6 mroute ff08::1:3 vrf green

VRF : green

Group Address      : ff08::1:3
Source Address     : 2001::03
Neighbor          : 2003::04
Incoming interface : 1/1/1
Outgoing Interface List :
Interface      State
-----
1/1/4          pruned
```

Showing information for group ff08::1:3 from source 2001::03 and all VRFs:

```
switch# show ipv6 mroute ff08::1:3 2001::03 all-vrfs

VRF : blue
```

```
Group Address      : ff08::1:3
Source Address     : 2001::03
Neighbor           : 2003::04
Incoming interface : 1/1/1
Outgoing Interface List :
Interface      State
-----
1/1/4         pruned
```

VRF : green

```
Group Address      : ff08::1:3
Source Address     : 2001::03
Neighbor           : 2003::04
Incoming interface : 1/1/2
Outgoing Interface List :
Interface      State
-----
1/1/4         pruned
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute

```
show ipv6 mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not

Parameter

Description

have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IPv6 mroute information for the default VRF:

```
Switch# show ipv6 mroute
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : ff32::10
Source Address     : fd00:192:168:20::2
SSM Mroute        : True
Neighbor          : fe80::f403:4301:1422:2600
Uptime            : 00:14:05
State             : route
Incoming interface : 1/1/5
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding
```

Showing IPv6 mroute information for all VRFs:

```
switch# do show ipv6 mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : ff32::10
Source Address     : fd00:192:168:2::100
SSM Mroute        : True
Neighbor          : fe80::eceb:b801:14e4:2900
Uptime            : 00:19:20
State             : route
Incoming interface : 1/1/4
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding

VRF : red
Total number of entries : 1

Group Address      : ff32::11
Source Address     : 30::3
SSM Mroute        : True
Neighbor          : fe80::eceb:b880:1fe4:2900
Uptime            : 00:01:13
State             : route
Incoming interface : vlan31
Outgoing Interface List :
```

Interface	State
-----	-----
vlan32	forwarding



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute brief

```
show ipv6 mroute brief [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows mroute information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 mroute brief:

```
switch# show ipv6 mroute brief all-vrfs
IP Multicast Route Entries

VRF : blu
Total number of entries : 2

Group Address   : ff08::1:3
Source Address  : 2002::04
```

```

Neighbor      : 2003::04
Interface     : 1/1/2

Group Address : ff08::1:4
Source Address : 2002::03
Neighbor      : 2003::05
Interface     : 1/1/3

VRF : default
Total number of entries : 1

Group Address : ff08::1:5
Source Address : 2001::03
Neighbor      : 2002::01
Interface     : 1/1/1

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6

`show ipv6 pim6 [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<code>all-vrfs</code>	Shows information for all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 PIM router:

```
switch# show ipv6 pim6

PIM Global Parameters

VRF                : default
PIM Status         : Enabled
Join/Prune Interval (sec) : 46
SPT Threshold      : Disabled
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 bsr

```
show ipv6 pim6 bsr [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about BSR candidates in the domain and multicast groups it supports. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing information about BSR candidates:

```
switch# show ipv6 pim6 bsr all-vrfs
```

Status and Counters- PIM-SM(IPv6) Bootstrap Router Information

```
VRF                                     : blu
E-BSR Address                         : 2006::06
E-BSR Priority                         : 0
E-BSR Hash Mask Length                : 0
E-BSR Up Time                         : 0 secs
Next Bootstrap Message                : 0 secs

C-BSR Admin Status                    : This system is a Candidate-BSR
C-BSR Address                         : 2007::01
C-BSR Priority                         : 40
C-BSR Hash Mask Length                : 36
C-BSR Message Interval                : 50
C-BSR Source IP Interface             : lag1

C-RP Admin Status                     : This system is a Candidate-RP
C-RP Address                         : 2007::01
C-RP Hold Time                        : 60
C-RP Advertise Period                 : 60
C-RP Priority                         : 46
C-RP Source IP Interface              : lag1

Group Prefix                          : ff00::/8
Group Prefix                          : ff08::1:3/64
Group Prefix                          : ff08::1:4/64

VRF                                     : default
E-BSR Address                         : 2001::01
E-BSR Priority                         : 40
E-BSR Hash Mask Length                : 36
E-BSR Up Time                         : 53 mins
Next Bootstrap Message                : 88 secs

C-BSR Admin Status                    : This system is a Candidate-BSR
C-BSR Address                         : 2001::01
C-BSR Priority                         : 40
C-BSR Hash Mask Length                : 36
C-BSR Message Interval                : 50
C-BSR Source IP Interface             : 1/1/1

C-RP Admin Status                     : This system is a Candidate-RP
C-RP Address                         : 2001::01
C-RP Hold Time                        : 60
C-RP Advertise Period                 : 60
C-RP Priority                         : 46
C-RP Source IP Interface              : 1/1/1

Group Prefix                          : ff00::/8
Group Prefix                          : ff08::1:5/64
Group Prefix                          : ff08::1:6/64
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

```
show ipv6 pim6 bsr elected
```

```
show ipv6 pim6 bsr elected [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows information about the elected BSR in the domain and multicast groups it supports. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM elected bootstrap router information:

```
switch# show ipv6 pim6 bsr elected all-vrfs

Status and Counters - PIM-SM(IPv6) Elected Bootstrap Router Information

VRF                                     : blu
E-BSR Address                         : 2005::05
E-BSR Priority                         : 0
E-BSR Hash Mask Length                : 0
E-BSR Up Time                         : 0 secs
Next Bootstrap Message                : 0 secs

VRF                                     : default
E-BSR Address                         : 2002::02
E-BSR Priority                         : 0
E-BSR Hash Mask Length                : 30
E-BSR Up Time                         : 50 mins
Next Bootstrap Message                : 88 secs
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 bsr local

```
show ipv6 pim6 bsr local [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about BSR candidates on the local router and multicast groups it supports. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing local Candidate BSR:

```
switch# show ipv6 pim6 bsr local all-vrfs

Status and Counters - PIM-SM(IPv6) Local Candidate-BSR Information

VRF                               : blu
C-BSR Admin Status                : This system is a Candidate-BSR
C-BSR Address                    : 2007::01
C-BSR Priority                    : 40
C-BSR Hash Mask Length           : 36
C-BSR Message Interval           : 50
C-BSR Source IP Interface        : lag1

VRF                               : default
C-BSR Admin Status                : This system is a Candidate-BSR
C-BSR Address                    : 2001::01
C-BSR Priority                    : 40
C-BSR Hash Mask Length           : 36
C-BSR Message Interval           : 50
C-BSR Source IP Interface        : 1/1/1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

```
show ipv6 pim6 interface <INTERFACE-NAME>
```

```
show ipv6 pim6 interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Parameter	Description
<INTERFACE-NAME>	Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface information for interface 1/1/1:

```
switch# show ipv6 pim6 interface 1/1/1

PIM Interfaces

VRF: default

Interface   : 1/1/1
IPv6 Address : fe80::a00:9ff:feec:dc0e/64
Mode        : sparse

Designated Router :
Hello Interval (sec) : 30
Hello Delay (sec)   : 4

Override Interval (msec) : 500
Propagation Delay (msec) : 350
Lan Prune Delay       : Yes
DR Priority            : 3
```

Neighbor Timeout : 0



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface

`show ipv6 pim6 interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface:

```
switch# show ipv6 pim6 interface
PIM Interfaces

VRF: default

Interface      IP Address
mode
-----
1/1/1          fe80::a00:9ff:feec:dc0e/64
```

sparse



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 neighbor

show ipv6 pim6 neighbor [<IPv6-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
<IPv6-ADDR>	Specifies a neighbor address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM neighbor information:

```
switch# show ipv6 pim6 neighbor

PIM Neighbor

VRF           : default
IP Address    : 2001::02
```

```
Interface          : 1/1/1
Up Time (sec)      : 0
Expire Time (sec)  : 0
DR Priority         : 44
```

Showing PIM neighbor information (including the presence of anycast neighbors) for all VRFs:

```
switch# show ipv6 pim6 neighbor all-vrfs

PIM Neighbor

VRF                  : red
Total number of neighbors : 2

IPv6 Address         : fe80::5:5:5:5
Interface            : vni10000
Up Time (HH:MM:SS)   : 06:57:07
Expire Time (HH:MM:SS) : 00:03:26
DR Priority           : 1
Hold Time (HH:MM:SS) : 00:03:30

IPv6 Address         : fe80::3821:c780:a5c:18c0
Interface            : vlan10
Up Time (HH:MM:SS)   : 00:01:46
Expire Time (HH:MM:SS) : 00:01:29
DR Priority           : 1
Hold Time (HH:MM:SS) : 00:01:45
Secondary IP Addresses :100:100::3
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 pending

```
show ipv6 pim6 pending [<GROUP-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the pending joins on a PIM router. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Use this command to determine what flows are being requested on the PIM network. If data availability for a flow is expected, and a join for the flow is pending, the troubleshooting search moves to the source of that flow, since the routers are verified to be seeing the request for data.

Parameter	Description
<code><GROUP-ADDR></code>	Specifies a group address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<code>all-vrfs</code>	Shows information for all VRFs.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing pending PIM joins:

```
switch# show ipv6 pim6 pending
Join Pending

VRF : default
  Group ff08::1:3
    (*,G) Pending
      Incoming Interface: 1/1/1
  Group ff08::1:4
    (*,G) Pending
      Incoming Interface: 1/1/1
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp

```
show ipv6 pim6 rp [<group-ip>] [{vrf <vrf-name>}|all-vrfs]
```

Description

Displays the rendezvous point (RP) address for a particular group in the given VRF. The output of this command also includes the type of RP (static or dynamic) and the uptime for the mapping. This information can help verify that Group-to-RP mapping is consistent across all routers in the network. If the **group-ip** parameter is not included, the output of this command displays the group-to-RP mappings of those groups with active multicast traffic in the given VRF. If a VRF name is not specified, the output of this command displays information for the default VRF.

Parameter	Description
<group-ip>	Display group-to-RP mappings for the specified group.
vrf <VRF-NAME>	Specifies the name of a VRF. The default VRF is named default .
all-vrfs	Selects all VRFs.

Example

Showing RP mapping information for a single group:

```
switch# show ipv6 pim6 rp ff57::3

VRF: default

PIM-SM(IPv6) Group-to-Resultant_RP Mapping Information

Group Address      : ff57::3
RP Address         : Not Found
RP Type            : -
Up Time (HH:MM:SS) : -
```

Showing RP mapping for all VRFs:

```
switch# show ipv6 pim6 rp all-vrfs

VRF: default

PIM-SM(IPv6) Group-to-Resultant_RP Mapping Information

Group Address      : ff56::7
RP Address         : 2002::2
RP Type            : bsr
Up Time (HH:MM:SS) : 00:45:20

VRF: red

PIM-SM(IPv6) Group-to-Resultant_RP Mapping Information

Group Address      : ff55::5
RP Address         : 4001::1
RP Type            : static
Up Time (HH:MM:SS) : 02:33:50

Group Address      : ff55::6
RP Address         : 3003::3
RP Type            : bsr
Up Time (HH:MM:SS) : 01:30:05
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rpf

show ipv6 pim6 rpf [<source-ip-address> [<group-ip-address>]] [vrf <vrf-name> | all-vrfs]

Description

Shows PIM RPF details for the specified source or RP address in the given VRF. It shows the nexthop and interface through which shortest path to the source is available. Additionally, it prints if PIM neighborship is present on the nexthop. If VRF is not given, it displays for default VRF.

Parameter	Description
<IP-ADDR>	Show PIM RPF details for the given IPv4/IPv6 (X:X::X:X) address
vrfs	Shows PIM RPF information for specific VRF.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
all-vrfs	Shows PIM RPF details in all VRFs.

Examples

Showing PIM RPF for VRF red:

```
switch# show ipv6 pim6 rpf vrf red

Multicast RPF Details
Origin Codes: C - connected, SM - static-multicast, SU - static-unicast
               O - OSPF, B - BGP, R - RIP
VRF: red
IP Address      : 2000::2
RPF Interface   : vlan20
RPF Nexthop     : -
PIM Neighbor    : no
RPF Route/Mask  : 2000::2/128
Origin          : C
In Use          : yes
```



```
IP Address       : 2222::2
RPF Interface    : vlan20
RPF Nexthop      : fe80::94f1:2880:141d:a800
PIM Neighbor     : yes
RPF Route/Mask   : 2222::2/128
Origin          : O
In Use           : yes
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-candidate

```
show ipv6 pim6 rp-candidate [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the candidate RP operational and configuration information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP candidate:

```
switch# show ipv6 pim6 rp-candidate all-vrfs

Status and Counters- PIM-SM(IPv6) Candidate-RP Information
```

```

VRF                               : blu
C-RP Admin Status                 : This system is a Candidate-RP
C-RP Address                      : 2007::01
C-RP Hold Time                   : 60
C-RP Advertise Period            : 60
C-RP Priority                     : 46
C-RP Source IP Interface         : lag1

Group Prefix                      : ff00::/8
Group Prefix                      : ff08::1:3/64
Group Prefix                      : ff08::1:4/64

VRF                               : default
C-RP Admin Status                 : This system is a Candidate-RP
C-RP Address                      : 2001::01
C-RP Hold Time                   : 60
C-RP Advertise Period            : 60
C-RP Priority                     : 46
C-RP Source IP Interface         : 1/1/1

Group Prefix                      : ff00::/8
Group Prefix                      : ff08::1:5/64
Group Prefix                      : ff08::1:6/64

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rpf-override

```
show ipv6 pim6 rpf-override [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the RPF override configuration, which can be useful information when troubleshooting potential RPF misconfigurations. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RPF override:

```
switch# show ipv6 pim6 rpf-override all-vrfs

VRF : Green
Static RPF Override
Multicast Source : 2003::1/128
RPF IPv6 Address : 2001::01
Multicast Source : 2005::1/128
RPF IPv6 Address : 2007::01
VRF : Red
Static RPF Override
Multicast Source : 2004::02/128
RPF IPv6 Address : 2002::02
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-registered-source

```
show ipv6 pim6 rp-registered-sources all-vrfs
```

Description

Displays the registered sources information on the RP router. This command shows information about the active multicast flows that are registered by the source designated router (DR) to this Rendezvous Point (RP). When the multicast source becomes inactive, the entry will be removed from this table. Note

that this command displays only the set of flows that have been registered successfully for which the current router is the RP.

show ipv6 pim6 rp registered sources

```
show ipv6 pim6 rp-registered-sources <group-address> [source-address] [all-vrfs | vrf <vrf-name>]
```

Description

Shows information about active multicast flows that are registered by source DR to a specific RP.

Parameter	Description	
<group-address>	Shows registered sources information for the group address. Format: X:X::X:X	Shows registered sources information for the group address
<source-address>	(Optional) Shows registered sources information for the group from this source. Format :X:X::X:X	Shows registered sources information for the group from selected source.
vrf <VRF-NAME>	Displays registered sources information for a specific VRF.	
all-vrfs	Displays registered sources information for all VRFs.	Shows registered sources information on all VRFs
vrf	Shows registered sources information for specific VRF	
vrf-name	Shows registered sources information for the given VRF	

Example

Showing information about rp-registered-sources in all-vrfs:

```
switch# show ipv6 pim6 rp-registered-sources all-vrfs
```

```
Multicast flows registered with this RP
```

```
VRF : default
```

```
Total number of entries : 1
```

Source Address	Group Address	RP Address
2001::1	ff55::5	2002::2

```
Multicast flows registered with this RP
```

```
VRF : red
```

```
Total number of entries : 1
```

Source Address	Group Address	RP Address

3001::1

ff99::5

3002::2

The following example shows the registered sources information for a specific group and source address.

```
switch# show ipv6 pim6 rp-registered-sources ff55::5 2001::1
```

Multicast flows registered with this RP

VRF : default

Total number of entries : 1

Source Address

Group Address

RP Address

2001::1

ff55::5

3333::3



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rpf-override source

```
show ipv6 pim6 rpf-override source <IPv6-ADDR> [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the RPF override configuration for the specified source. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
source <IPv6-ADDR>	Specifies the RPF source address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing PIM RPF override source:

```
switch# show ipv6 pim6 rpf-override source 2004::02

VRF : default
Static RPF Override
Multicast Source : 2004::02/128
RPF IPv6 Address : 2002::02
```

Showing PIM RPF override source for all VRFs:

```
switch# show ipv6 pim6 rpf-override source 2004::02 all-vrfs

VRF : Red
Static RPF Override
Multicast Source : 2004::02/128
RPF IPv6 Address : 2002::02
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-set

```
show ipv6 pim6 rp-set [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for both the learned C-RP assignments and any statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set information:

```
switch# show ipv6 pim6 rp-set all-vrfs

VRF: blu

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix   : ff00::/8
RP Address     : 2004::04
Override [No]  : No

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information

Group Prefix   : ff08::1:3/64
RP Address     : 2007::01
Hold Time (sec) : 60
Expire Time (sec) : 0
Group Prefix   : ff08::1:4/64
RP Address     : 2007::01
Hold Time (sec) : 60
Expire Time (sec) : 92

VRF: default

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix   : ff00::/8
RP Address     : 2003::03
Override [No]  : No

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information

Group Prefix   : ff08::1:5/64
RP Address     : 2001::01
Hold Time (sec) : 60
Expire Time (sec) : 0
Group Prefix   : ff08::1:6/64
RP Address     : 2002::01
Hold Time (sec) : 60
Expire Time (sec) : 92
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-set learned

```
show ipv6 pim6 rp-set learned [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for dynamically learned RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set learned information:

```
switch# show ipv6 pim6 rp-set learned all-vrfs

VRF: blu

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information
Group Prefix      : ff08::1:3/64
RP Address        : 2007::01
Hold Time (sec)   : 60
Expire Time (sec) : 0
Group Prefix      : ff08::1:4/64
RP Address        : 2007::01
Hold Time (sec)   : 60
Expire Time (sec) : 92

VRF: default

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information
Group Prefix      : ff08::1:5/64
RP Address        : 2001::01
Hold Time (sec)   : 60
```



```
Expire Time (sec) : 0
Group Prefix      : ff08::1:6/64
RP Address        : 2002::01
Hold Time (sec)   : 60
Expire Time (sec) : 92
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-set static

```
show ipv6 pim6 rp-set static [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM Static RP set information:

```
switch# show ipv6 pim6 rp-set static all-vrfs

VRF: blu

Status and Counters - PIM-SM(IPv6) Static RP-Set Information
```

```

Group Prefix   : ff00::/8
RP Address     : 2004::04
Override [No]  : No

VRF: default

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix   : ff00::/8
RP Address     : 2003::03
Override [No]  : No

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 tree-state

```
show ipv6 pim6 tree-state {<group-ip> [<source-ip>]}|brief [{vrf <vrf-name>}]| all-vrfs]
```

Description

Displays upstream join states for a specified group and source address in a VRF in an IPv6 network.

The command displays upstream state, upstream interface and RPF neighbor used to send join messages and a list of downstream interfaces from which join messages are received.

The set of downstream interfaces in this command may not show the final list of outgoing interfaces for a flow, which is computed from various internal states and is shown in the output of the command [show ipv6 mroute](#).

Parameter	Description
<group-ip>	Shows PIM Join details for the specified group IPv6 address
<source-ip>	Shows PIM Join details for the specified source IPv6 address. If a source address is not specified, only *,G states are displayed for the specified group. If a source address is specified, (S,G) states are displayed along with (*,G) states and (S,G,RPT) states wherever

Parameter	Description
	applicable.
brief	Display brief details for the multicast group and source in a table format.
vrf <VRF-NAME>	Show join state details for the specified VRF.
all-vrfs	Show join state details for all VRFs.

Usage

The output of this command can indicate one of the following two multicast group (*,G) and multicast source and group (S,G) upstream states:

- **Joined** : Join sent to upstream RPF neighbor.
- **Not Joined** : Joins not sent upstream.

The following states are applicable to the multicast group (*,G), and root path tree (S,G,RPT) only:

- **Pruned** : Traffic from the source is arriving on the shortest path tree, (*,G) Joined, but (S,G,RPT) pruned.
- **Not Pruned** : Traffic from the multicast group (*,G) Joined, and (S,G,rpt) not pruned.
- **RPT Not Joined** : The multicast group (*,G) has not joined.

Examples

Display multicast group (*,G) join information for the VRF **red**.

```
show ipv6 pim6 tree-state ff55::1 vrf red
(*,G) Information for Group ff55::1
VRF: red
Upstream Information:
State                : Joined
Joined Interface     : vlan50
RPF Neighbor         : 20::2
Uptime               : 01:58:30
Downstream Information:
Interfaces           : vlan50, vlan201
```

Display group (*,G), source and group (S,G), and root-path tree (S,G, RPT) Information for group **ff55::1** and source IP **30::1**.

```
show ipv6 pim6 tree-state ff55::1 30::1 vrf red
(*,G) Information for Group ff55::1
VRF: red
Upstream Information:
State                : Joined
Joined Interface     : vlan50
RPF Neighbor         : 20::2
Uptime               : 01:58:30
Downstream Information:
Interfaces           : vlan200
(S,G) Information for Group ff55::1 Source 30::1
Upstream Information:
```

```

State                               : Joined
Joined Interface                     : vlan30
RPF Neighbor                         : 40::2
Uptime                              : 01:57:30
SPT bit set                         : True
Downstream Information:
Interfaces                           : vlan200
(S,G,RPT) Information for Group ff55::1 Source 30::1
Upstream Information:
State                               : Pruned
Joined Interface                     : vlan50
RPF Neighbor                         : 20::2
Uptime                              : 01:58:30
Downstream Information:
Interfaces                           : vlan200

```

Display brief information for the IPv6 PIM6 tree state.

```

show ipv6 pim6 tree-state brief
State abbreviations :
J - Joined  NJ - Not Joined  RPTNJ - RPT Not Joined
P - Pruned  NP - Not Pruned
-----
VRF : default
-----
Group Address      Source Address      RPF      Uptime      State  Type
Neighbor          (HH:MM:SS)
-----
ff5e::1            *                    10::2    01:58:30    J      *,G
ff5e::1            2035:135:1::100    10::2    01:58:30    J      S,G
ff5e::2            *                    10::2    01:58:30    J      *,G
ff5e::2            2035:135:1::100    20::2    01:58:30    J      S,G
ff5e::2            2035:135:1::100    10::2    01:58:30    P      S,G,RPT
-----

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.14	-Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

sources-per-group

`sources-per-group <limit>`

```
no sources-per-group <limit>
```

Description

Configures the total number of sources allowed for a group on the router. By default, there is no limit on the number of sources for a group. When the number of sources for a group exceeds the configured limit, multicast traffic from additional sources will be dropped.

The **no** form of this command removes the currently configured limit value.

Parameter	Description
<code><limit></code>	Specifies the value to be configured as the sources allowed per group. Range: 1 to 4294967295.

Usage

Flows exceeding the limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration does not allow new sources for the group. At the time of configuration, if the device has more sources for the given group than the configured value, already allowed sources continue to exist until they are removed.

The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage.

Examples

Configuring and removing the sources allowed per group:

```
switch(config)# router pim6
switch(config-pim6)# sources-per-group 4
switch(config-pim6)# no sources-per-group
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced for IPv6

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

spt-threshold

```
spt-threshold
no spt-threshold
```

Description

Enables the router to switch the multicast traffic flows to the shortest path tree. Default is enabled. The **no** form of this command disables the routers ability to switch the multicast traffic flows to the shortest path tree.

To apply this configuration a user needs to apply disable/enable PIM globally.

Example

Enabling and disabling the SPT threshold:

```
switch(config)# router pim6  
switch(config-pim6)# spt-threshold  
switch(config-pim6)# no spt-threshold
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

ip igmp apply ssm-map access-list

```
ip igmp apply ssm-map access-list<ACL-NAME>
no ip igmp apply ssm-map access-list<ACL-NAME>
```

Description

Configures SSM-map ACL on a specific interface.

The **no** form of this command removes the currently configured ACL rule.



Existing classifier commands are used to configure ACL.

Parameter	Description
<ACL-NAME>	Required. Specifies the ACL rule name.

Restrictions

- ACE using mask for source address will be ignored.
- ACE must include unicast source (address/source group) and multicast destination (address/destination group) as matching criteria. Entries using "any" for source address or destination address will be ignored.
- IGMPv3/MLDv2 dynamic joins will be ignored for groups in SSM-map (SSM-map is higher priority).

Usage

- When configured, every incoming IGMPv2/v1 join packet sent to the SSM range group address is converted to (S, G) channels where S is the source address specified in the SSM-map ACL.
- Object-groups can be used to group multiple sources or multiple destination addresses.

Recommendations related to SSM-map:

- Interfaces with SSM-map configured should use version 3 for IGMP and version 2 for MLD. If older versions are used, sources will not be learned.
- If SSM-map configuration is dynamically changed by adding or deleting sources associated with a group, the change will take effect when the next incoming join packet is received.
- SSM-map configuration must be consistent across all L3 nodes in the network.
- Multiple ACEs with same destination (address/destination object group) are not recommended as only the first match will be implemented. If a group must be mapped with multiple sources, source object group can be used instead of having multiple ACEs with the same destination match.

Examples

Creating SSM map ACL:

```
switch(config)# access-list ip SSM_MAP
switch(config-acl-ip)# permit ip 30.1.1.1 232.1.1.1
switch(config-acl-ip)# permit ip 20.1.1.1 232.1.1.2
```

Applying SSM_MAP ACL on a SVI:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp apply ssm-map access-list SSM_MAP
```

Creating SSM map ACL using object groups:

```
switch(config)# object-group ip address source-group
switch(config-addrgroup-ip)# 10.1.1.1
switch(config-addrgroup-ip)# 10.1.1.2
switch(config)# object-group ip address destination-group
switch(config-addrgroup-ip)# 232.2.1.1
switch(config-addrgroup-ip)# 232.3.1.1
switch(config)# access-list ip SSM_MAP_OB
switch(config-acl-ip)# permit ip source-group 232.1.1.3
switch(config-acl-ip)# permit ip 20.1.1.1 destination-group
```

In the above configuration:



- When lower version joins are received for group 232.1.1.3, they will be converted to (S,G) channels (10.1.1.1, 232.1.1.3) and (10.1.1.2, 232.1.1.3).
- When lower version joins are received from group 232.2.1.1 and 232.3.1.1, they will be converted to (S, G) channels (20.1.1.1, 232.2.1.1) and (20.1.1.1, 232.3.1.1)

Applying SSM_MAP_OB ACL on a SVI:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# ip igmp apply ssm-map access-list SSM_MAP_OB
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

show ip igmp ssm-map

```
show ip igmp [ssm-map [vrf <VRF-NAME> | all-vrfs]]
```


Description

Shows IGMP SSM map.

Parameter	Description
<code><VRF-NAME></code>	(Optional) Shows SSM map in a specific VRF.
<code>all-vrfs</code>	(Optional) Shows SSM map in all VRFs.

Examples

Showing IGMP SSM map:

```
switch# show ip igmp ssm-map
IGMP SSM-map Information
VRF Name      :default
Interface Name  SSM-map ACL name
-----
vlan10         ssm-map-1
vlan20         ssm-map-2
1/1/1         ssm-map-1
2/1/1.1       ssm-map-3
```

Showing IGMP SSM map for all VRFs:

```
switch# show ip igmp ssm-map all-vrfs
IGMP SSM-map Information
VRF Name      :test
Interface Name  SSM-map ACL name
-----
vlan30         ssm-map-1
VRF Name      :default
Interface Name  SSM-map ACL name
-----
vlan10         ssm-map-1
vlan20         ssm-map-2
1/1/1         ssm-map-1
2/1/1.1       ssm-map-3
```

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

pim-ssm

pim-ssm
no pim-ssm

Description

Enables PIM source-specific multicast globally on the router. When PIM SSM is enabled, the RP configuration is ignored/ not required for a particular range of multicast addresses.

The **no** form of this command disables PIM-SSM globally on the router.

When PIM-SSM is enabled for the SSM range for multicast groups, the following behavior is observed:

- PIM joins and prunes are directly sent towards the source. No (*,G) joins or prunes are sent towards RP.
- Only IGMPv3/MLDv2 joins with source include filter are considered for SSM.

Usage

- PIM-SSM is recommended to be configured only on the last hop router or receiver DR if the topology contains a combination of IGMPv2 and IGMPv3, or MLDv1 and MLDv2, clients.
- Configuring or unconfiguring PIM SSM can lead to momentary traffic loss until PIM rebuilds the states.
- PIM-SSM is not supported with VxLAN.

Example

Enabling PIM-SSM on the router:

```
switch(config)# router pim  
switch(config-pim)# pim-ssm
```

Disabling PIM-SSM on the router:

```
switch(config)# router pim  
switch(config-pim)# no pim-ssm
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

pim-ssm range-access-list

```
pim-ssm range-access-list <ACL-RULE>
no pim-ssm range-access-list <ACL-RULE>
```

Description

Enables the PIM router to modify the default SSM range. The IPv4 default PIM-SSM group range is 232.0.0.0/8.

The **no** form of this command removes the currently configured ACL rule.

Parameter	Description
<ACL-RULE>	(Required) Specifies the ACL rule name.

Usage

- In the ACL used to specify the PIM-SSM range, ACEs should contain only multicast group addresses in the destination IP field, else the ACE is ignored.
- Modifying the PIM-SSM range can lead to momentary traffic loss until PIM rebuilds the states.
- It is recommended to keep the SSM range the same across the network.

Examples

Creating an IPv4 ACL named **pim_ssm_grp_range_acl** and applying the ACL as a PIM-SSM range ACL:

```
switch# configure terminal
switch(config)# access-list ip pim_ssm_grp_range_acl
switch(config-acl-ip)# 10 permit any any 225.1.1.2/255.255.255.0
switch(config-acl-ip)# 20 permit any any 239.1.1.2/255.255.255.0

switch(config)# router pim
switch(config-pim)# pim-ssm range-access-list pim_ssm_grp_range_acl
switch(config-pim)# pim-ssm range-access-list pim_ssm_grp_range_acl 1
Failed to configure PIM-SSM Range ACL. ACL pim_ssm_grp_range_acl_1 does not exist.
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim	Administrators or local user group members with execution rights for this command.

show ip mroute

```
show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows mroute information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP mroute for the default VRF:

```
Switch(config-vlan-20)# show ip mroute
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : 232.10.10.10
Source Address     : 192.168.20.2
SSM Mroute         : True
Neighbor           : 192.168.3.0
Uptime             : 02:08:31
State               : route
Incoming interface : 1/1/5
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding
```

Showing IP mroute for all VRFs:

```

switch# do show ip mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : 232.10.10.10
Source Address     : 192.168.2.100
SSM Mroute         : True
Neighbor           : 192.168.3.0
Uptime             : 00:38:24
State               : route
Incoming interface  : 1/1/4
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding

VRF : red
Total number of entries : 1

Group Address      : 232.11.11.11
Source Address     : 30.0.0.3
SSM Mroute         : True
Neighbor           : 31.0.0.1
Uptime             : 00:32:55
State               : route
Incoming interface  : vlan31
Outgoing Interface List :
Interface          State
-----
vlan32             forwarding

switch#

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip multicast summary

```
show ip multicast summary
```

Description

Displays multicast summary information.

Example

Showing multicast summary information:

```
Switch# show ip multicast summary

Total number of IGMP interfaces                : 1
Total number of IGMP snooping VLANs           : 0
Total number of IGMP joins                     : 1
Total number of IGMP snooping joins            : 0
Total number of PIM SM enabled VRFs            : 1
Total number of PIM SSM enabled VRFs           : 1
Total number of PIM DM enabled VRFs           : 0
Total number of PIM SM interfaces              : 2
Total number of PIM DM interfaces              : 0
Total number of PIM SM neighbors               : 1
Total number of PIM DM neighbors               : 0
Total number of PIM A/A enabled VRF           : 0
Total number of PIM A/A enabled interfaces     : 0
Total number of PIM SM Mroutes in route state  : 1
Total number of PIM SM Mroutes in bridge state : 0
Total number of PIM SSM Mroutes in route state : 1
Total number of PIM SSM Mroutes in bridge state : 0
Total number of PIM DM Mroutes in route state  : 0
Total number of PIM DM Mroutes in bridge state : 0
Total number of local multicast flows registered in this RP : 0
Total number of MLD interfaces                 : 1
Total number of MLD snooping VLANs            : 1
Total number of MLD joins                     : 1
Total number of MLD snooping joins            : 1
Total number of PIMv6 SM enabled VRFs          : 1
Total number of PIMv6 SSM enabled VRFs         : 0
Total number of PIMv6 DM enabled VRFs         : 0
Total number of PIMv6 SM interfaces            : 2
Total number of PIMv6 DM interfaces            : 0
Total number of PIMv6 SM neighbors             : 1
Total number of PIMv6 DM neighbors             : 0
Total number of PIMv6 A/A enabled VRF         : 0
Total number of PIMv6 A/A enabled interfaces   : 0
Total number of PIMv6 SM Mroutes in route state : 1
Total number of PIMv6 SM Mroutes in bridge state : 0
Total number of PIMv6 SSM Mroutes in route state : 1
Total number of PIMv6 SSM Mroutes in bridge state : 0
Total number of PIMv6 DM Mroutes in route state : 0
Total number of PIMv6 DM Mroutes in bridge state : 0
Total number of MSDP peers                     : 0
Total number of SA's learned by MSDP          : 0

VRF: default
Total number of IGMP interfaces                : 1
Total number of IGMP snooping VLANs           : 0
Total number of IGMP joins                     : 1
Total number of IGMP snooping joins            : 0
Total number of PIM SM interfaces              : 2
Total number of PIM DM interfaces              : 0
Total number of PIM SM neighbors               : 1
Total number of PIM DM neighbors               : 0
Total number of PIM A/A enabled interfaces     : 0
Total number of PIM SM Mroutes in route state  : 1
Total number of PIM SM Mroutes in bridge state : 0
Total number of PIM SSM Mroutes in route state : 1
```

```

Total number of PIM SSM Mroutes in bridge state      : 0
Total number of PIM DM Mroutes in route state       : 0
Total number of PIM DM Mroutes in bridge state      : 0
Total number of local multicast flows registered in this RP : 0
Total number of MLD interfaces                      : 1
Total number of MLD snooping VLANs                 : 1
Total number of MLD joins                          : 1
Total number of MLD snooping joins                 : 1
Total number of PIMv6 SM interfaces                : 2
Total number of PIMv6 DM interfaces                : 0
Total number of PIMv6 SM neighbors                 : 1
Total number of PIMv6 DM neighbors                 : 0
Total number of PIMv6 A/A enabled interfaces       : 0
Total number of PIMv6 SM Mroutes in route state    : 1
Total number of PIMv6 SM Mroutes in bridge state   : 0
Total number of PIMv6 SSM Mroutes in route state   : 1
Total number of PIMv6 SSM Mroutes in bridge state   : 0
Total number of PIMv6 DM Mroutes in route state    : 0
Total number of PIMv6 DM Mroutes in bridge state    : 0
Total number of MSDP peers                        : 0
Total number of SA's learned by MSDP               : 0

Switch#

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name counters

show ip pim interface <INTERFACE-NAME> counters [vsx-peer]

Description

Shows the PIM packet counters information for the specified interface.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to show packet counter information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the

Parameter	Description
	VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Example

Showing PIM packet counters for interface 1/1/5:

```
Switch(config)# show ip pim interface 1/1/5 counters
```

```
Interface   : 1/1/5
VRF         : default
```

Tx Counters :

Hello	310
State Refresh	0
Join/Prune	141
SSM Join/Prune	141
RP Advertisement	0
Graft	0
Graft Ack	0
Assert	0
Bsm	0
Register	0
Register Stop	0
SSM Register Stop	0

Rx Counters :

Hello	308
State Refresh	0
Join/Prune	0
SSM Join/Prune	0
RP Advertisement	0
Graft	0
Graft Ack	0
Assert	0
Bsm	0
Register	0
SSM Register	0
Register Stop	0
Register Drops(Register ACL hitcount)	0
Join/Prune Drops(RP ACL hitcount)	0

Rx Drop Counters :

Hello	0
State Refresh	0
Join/Prune	0
RP Advertisement	0
Graft	0


```
Graft Ack          0
Assert             0
Bsm                0
Switch(config) #
```

Showing PIM packet counters for interface VLAN 1:

```
switch# show ip pim interface vlan1 counters

Interface          : vlan1
VRF                 : default

Rx Counters :

Hello              4
State Refresh      0
Join/Prune         1
RPadv              0
Graft              0
GraftAck           0
Assert             0
Bsm                0
Register           0
Register Stop      0
Register Drops(Register ACL hitcount) 10
Join/Prune Drops(RP ACL hitcount)      5

Tx Counters :

Hello              9
State Refresh      0
Join/Prune         0
RPadv              0
Graft              0
GraftAck           0
Assert             0
Bsm                0
Register           0
Register Stop      0

Invalid Rx Counters :

Hello              0
State Refresh      0
Join/Prune         0
RPadv              0
Graft              0
GraftAck           0
Assert             0
Bsm                0
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ipv6 mld apply ssm-map access-list

```
ipv6 mld apply ssm-map access-list <ACL-NAME>
no ipv6 mld apply ssm-map access-list <ACL-NAME>
```

Description

Configures SSM-map ACL on a specific interface.

The **no** form of this command removes the currently configured ACL.



Existing classifier commands are used to configure ACL.

Parameter	Description
<ACL-NAME>	Required. Specifies the ACL name.

Restrictions

- ACE using mask for source address will be ignored.
- ACE must include unicast source (address/source group) and multicast destination (address/destination group) as matching criteria. Entries using "any" for source address or destination address will be ignored.
- IGMPv3/MLDv2 dynamic joins will be ignored for groups in SSM-map (SSM-map is higher priority).

Usage

- When configured, every incoming MLDv1 join packet sent to the same SSMv6 range group address is converted to (S, G) channels where S is the source address specified in the SSM-map ACL.
- Object-groups can be used to group multiple sources or multiple destination addresses.

Recommendations related to SSM-map:

- Interfaces with SSM-map configured should use version 3 for IGMP and version 2 for MLD. If older versions are used, sources will not be learned.
- If SSM-map configuration is dynamically changed by adding or deleting sources associated with a group, the change will take effect when the next incoming join packet is received.
- SSM-map configuration must be consistent across all L3 nodes in the network.
- Multiple ACEs with same destination (address/destination object group) are not recommended as only the first match will be implemented. If a group must be mapped with multiple sources, source object group can be used instead of having multiple ACEs with the same destination match.

Examples

Creating SSM map v6 ACL:

```
switch(config)# access-list ipv6 SSM_MAP_V6
switch(config-acl-ip)# permit ipv6 2003::1 ff34::1
switch(config-acl-ip)# permit ipv6 2002::1 ff36::1
switch(config-acl-ip)# exit
```

Applying SSM_MAP_V6 ACL on SVI 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld apply ssm-map access-list SSM_MAP_V6
```

Creating SSM map V6 ACL with object groups:

```
switch(config)# object-group ipv6 address source-group-ipv6
switch(config-addrgroup-ipv6)# 2001::1
switch(config-addrgroup-ipv6)# 2001::2
switch(config)# object-group ipv6 address destination-group-ipv6
switch(config-addrgroup-ipv6)# ff31::1
switch((config-addrgroup-ipv6)# ff32::1
switch(config)# access-list ipv6 SSM_MAP_V6_OB
switch(config-acl-ip)# permit ipv6 source-group-ipv6 ff36::1
switch(config-acl-ip)# permit ipv6 2004::1 destination-group-ipv6
```

Applying SSM_MAP_V6_OB ACL on SVI 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# ipv6 mld apply ssm-map access-list SSM_MAP_V6_OB
```

In the above configuration:



- When lower version joins are received for group ff36::1, they will be converted to (S, G) channels (2001::1, ff36::1) and (2001::2, ff36::1).
- When lower version joins are received for group ff31::1 and ff32::1, they will be converted to (S, G) channels (2003::1, ff31::1) and (2003::1, ff32::1).

Command History

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-if-vlan	Administrators or local user group members with execution rights for this command.

pim-ssm

pim-ssm

```
no pim-ssm
```

Description

Enables PIM-SSM globally on the router. When PIM-SSM is enabled, the RP configuration is ignored/ not required for a particular range of multicast addresses.

The **no** form of this command disables PIM-SSM globally on the router.

When PIM-SSM is enabled for the SSM range for multicast groups, the following behavior is observed:

- PIM joins and prunes are directly sent towards the source. No (*,G) joins or prunes are sent towards RP.
- Only IGMPv3/MLDv2 joins with source include filter are considered for SSM.

Usage

- PIM-SSM is recommended to be configured only on the last hop router or receiver DR if the topology contains a combination of IGMPv2 and IGMPv3, or MLDv1 and MLDv2, clients.
- Configuring or unconfiguring PIM SSM can lead to momentary traffic loss until PIM rebuilds the states.
- PIM-SSM is not supported with VxLAN.

Example

Entering the PIMv6 configuration context and enabling PIM-SSM on the router:

```
switch(config)# router pim6
switch(config-pim6)# pim-ssm
```

Disabling PIM-SSM on the router:

```
switch(config)# router pim6
switch(config-pim6)# no pim-ssm
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

pim-ssm range-access-list

```
pim-ssm range-access-list <ACL-RULE>
```

```
no pim-ssm range-access-list <ACL-RULE>
```

Description

Enables the PIM router to modify the default SSM range. The IPv6 default PIM-SSM group range is FF3x::/32.

The **no** form of this command removes the currently configured ACL rule.

Parameter	Description
<ACL-RULE>	Required. Specifies the ACL rule name.

Usage

- In the ACL used to specify the PIM-SSM range, ACEs should contain only multicast group addresses in the destination IP field, else the ACE will be ignored.
- Modifying the PIM-SSM range can lead to momentary traffic loss until PIM rebuilds the states.
- It is recommended to keep the SSM range the same across the network.

Examples

Creating an IPv6 ACL named **pim_ssm_v6grp_range_acl** with two entries and applying the ACL as a PIM-SSM range ACL:

```
switch# configure terminal
switch(config-pim)# access-list ipv6 pim_ssm_v6grp_range_acl
switch(config-acl-ipv6)# 10 permit any any ff2e::2/64
switch(config-acl-ipv6)# 20 permit any any ff1e::1/64

switch(config)# router pim6
switch(config-pim6)# pim-ssm range-access-list pim_ssm_v6grp_range_acl
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-pim6	Administrators or local user group members with execution rights for this command.

show ip multicast summary

```
show ip multicast summary
```

Description

Displays multicast summary information.

Example

Showing multicast summary information:

```
Switch# show ip multicast summary

Total number of IGMP interfaces                : 1
Total number of IGMP snooping VLANs           : 0
Total number of IGMP joins                     : 1
Total number of IGMP snooping joins           : 0
Total number of PIM SM enabled VRFs            : 1
Total number of PIM SSM enabled VRFs          : 1
Total number of PIM DM enabled VRFs           : 0
Total number of PIM SM interfaces              : 2
Total number of PIM DM interfaces              : 0
Total number of PIM SM neighbors               : 1
Total number of PIM DM neighbors               : 0
Total number of PIM A/A enabled VRF           : 0
Total number of PIM A/A enabled interfaces     : 0
Total number of PIM SM Mroutes in route state : 1
Total number of PIM SM Mroutes in bridge state : 0
Total number of PIM SSM Mroutes in route state : 1
Total number of PIM SSM Mroutes in bridge state : 0
Total number of PIM DM Mroutes in route state : 0
Total number of PIM DM Mroutes in bridge state : 0
Total number of local multicast flows registered in this RP : 0
Total number of MLD interfaces                 : 1
Total number of MLD snooping VLANs            : 1
Total number of MLD joins                     : 1
Total number of MLD snooping joins            : 1
Total number of PIMv6 SM enabled VRFs         : 1
Total number of PIMv6 SSM enabled VRFs        : 0
Total number of PIMv6 DM enabled VRFs         : 0
Total number of PIMv6 SM interfaces            : 2
Total number of PIMv6 DM interfaces            : 0
Total number of PIMv6 SM neighbors             : 1
Total number of PIMv6 DM neighbors             : 0
Total number of PIMv6 A/A enabled VRF         : 0
Total number of PIMv6 A/A enabled interfaces  : 0
Total number of PIMv6 SM Mroutes in route state : 1
Total number of PIMv6 SM Mroutes in bridge state : 0
Total number of PIMv6 SSM Mroutes in route state : 1
Total number of PIMv6 SSM Mroutes in bridge state : 0
Total number of PIMv6 DM Mroutes in route state : 0
Total number of PIMv6 DM Mroutes in bridge state : 0
Total number of MSDP peers                     : 0
Total number of SA's learned by MSDP          : 0

VRF: default
Total number of IGMP interfaces                : 1
Total number of IGMP snooping VLANs           : 0
Total number of IGMP joins                     : 1
Total number of IGMP snooping joins           : 0
Total number of PIM SM interfaces              : 2
Total number of PIM DM interfaces              : 0
Total number of PIM SM neighbors               : 1
Total number of PIM DM neighbors               : 0
Total number of PIM A/A enabled interfaces     : 0
Total number of PIM SM Mroutes in route state : 1
Total number of PIM SM Mroutes in bridge state : 0
Total number of PIM SSM Mroutes in route state : 1
```

```

Total number of PIM SSM Mroutes in bridge state      : 0
Total number of PIM DM Mroutes in route state       : 0
Total number of PIM DM Mroutes in bridge state      : 0
Total number of local multicast flows registered in this RP : 0
Total number of MLD interfaces                      : 1
Total number of MLD snooping VLANs                 : 1
Total number of MLD joins                          : 1
Total number of MLD snooping joins                 : 1
Total number of PIMv6 SM interfaces                : 2
Total number of PIMv6 DM interfaces                : 0
Total number of PIMv6 SM neighbors                 : 1
Total number of PIMv6 DM neighbors                 : 0
Total number of PIMv6 A/A enabled interfaces        : 0
Total number of PIMv6 SM Mroutes in route state    : 1
Total number of PIMv6 SM Mroutes in bridge state   : 0
Total number of PIMv6 SSM Mroutes in route state   : 1
Total number of PIMv6 SSM Mroutes in bridge state   : 0
Total number of PIMv6 DM Mroutes in route state    : 0
Total number of PIMv6 DM Mroutes in bridge state    : 0
Total number of MSDP peers                         : 0
Total number of SA's learned by MSDP               : 0

Switch#

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim interface counters

`show ipv6 pim interface <INTERFACE-NAME> counters [vsx-peer]`

Description

Shows the PIM packet counters information for the specified interface.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface to show packet counter information.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the

Parameter	Description
	VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Example

Showing IPv6 PIM packet counters:

```
Switch#
Switch# show ipv6 pim interface 1/1/5 counters

Interface   : 1/1/5
VRF         : default

Tx Counters :

Hello                275
State Refresh        0
Join/Prune           32
SSM Join/Prune       32
RP Advertisement     0
Graft                0
Graft Ack            0
Assert               0
Bsm                  0
Register              0
Register Stop        0
SSM Register Stop    0

Rx Counters :

Hello                272
State Refresh        0
Join/Prune           0
SSM Join/Prune       0
RP Advertisement     0
Graft                0
Graft Ack            0
Assert               0
Bsm                  0
Register              0
SSM Register         0
Register Stop        0
Register Drops(Register ACL hitcount) 0
Join/Prune Drops(RP ACL hitcount)     0

Rx Drop Counters :

Hello                0
State Refresh        0
Join/Prune           0
RP Advertisement     0
```

```
Graft 0
Graft Ack 0
Assert 0
Bsm 0
Switch#
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld ssm-map

```
show ipv6 mld [ssm-map [vrf <VRF-NAME> | all-vrfs]]
```

Description

Shows MLD SSM map.

Parameter	Description
<VRF-NAME>	Optional. Shows MLD SSM map in a specific VRF.
<i>all-vrfs</i>	Optional. Shows MLD SSM map in all VRFs.

Examples

Showing MLD SSM-map:

```
switch# show ipv6 mld ssm-map
MLD SSM-map Information
VRF Name      :default
Interface Name  SSM map ACL name
-----
vlan10         ipv6-ssm-map-1
vlan20         ipv6-ssm-map-2
1/1/1         ipv6-ssm-map-3
2/1/1.1       ipv6-ssm-map-1
```

Showing MLD SSM-map for all VRFs:

```
switch# show ipv6 mld ssm-map all-vrfs
MLD SSM-map Information
VRF Name      :test
Interface Name  SSM map ACL name
-----
vlan30         ipv6-ssm-map-1
VRF Name      :default
Interface Name  SSM map ACL name
-----
vlan10         ipv6-ssm-map-1
vlan20         ipv6-ssm-map-2
1/1/1         ipv6-ssm-map-3
2/1/1.1       ipv6-ssm-map-1
```

Release	Modification
10.11	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ipv6 mroute

```
show ipv6 mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameter	Description
all-vrfs	Shows information for all VRFs.
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IPv6 mroute information for the default VRF:

```
Switch# show ipv6 mroute
IP Multicast Route Entries
```

```

VRF : default
Total number of entries : 1

Group Address      : ff32::10
Source Address     : fd00:192:168:20::2
SSM Mroute        : True
Neighbor          : fe80::f403:4301:1422:2600
Uptime            : 00:14:05
State             : route
Incoming interface : 1/1/5
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding

```

Showing IPv6 mroute information for all VRFs:

```

switch# do show ipv6 mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 1

Group Address      : ff32::10
Source Address     : fd00:192:168:2::100
SSM Mroute        : True
Neighbor          : fe80::eceb:b801:14e4:2900
Uptime            : 00:19:20
State             : route
Incoming interface : 1/1/4
Outgoing Interface List :
Interface          State
-----
vlan20             forwarding

VRF : red
Total number of entries : 1

Group Address      : ff32::11
Source Address     : 30::3
SSM Mroute        : True
Neighbor          : fe80::eceb:b880:1fe4:2900
Uptime            : 00:01:13
State             : route
Incoming interface : vlan31
Outgoing Interface List :
Interface          State
-----
vlan32             forwarding

```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ping

```
ping <IPv4-ADDR> | <hostname> [data-fill <pattern> | datagram-size <size> |  
    interval <time> | repetitions <number> | timeout <time> | tos <number> |  
    ip-option {include-timestamp | include-timestamp-and-address | record-route} |  
    vrf <vrfname> | do-not-fragment][source {IPv4-ADDR | IFNAME}]
```



Ping on VXLAN with ip-option such as include-timestamp-and-address, include-timestamp and record-route is not supported.

Description

Pings the specified IPv4 address or hostname with or without optional parameters.

Parameter	Description
ping <IPv4-ADDR>	Selects the IPv4 address to ping.
<HOSTNAME>	Selects the hostname to ping. Range: 1-256 characters
data-fill <PATTERN>	Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB
datagram-size <SIZE>	Specifies the ping datagram size. Range: 0-65399, default: 100.
interval <TIME>	Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.
repetitions <NUMBER>	Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.
timeout <TIME>	Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.
tos <NUMBER>	Specifies the IP Type of Service to be used in Ping request. Range: 0-255
ip-option {include-timestamp include-timestamp-and-address record-route}	Specifies an IP option (record-route or timestamp option).
include-timestamp	Specifies the intermediate router time stamp.
include-timestamp-and-address	Specifies the intermediate router time stamp and IP address.
record-route	Specifies the intermediate router addresses.

Parameter	Description
vrf <VRF-NAME>	Specifies the virtual routing and forwarding (VRF) to use. When VRF option is not given, the default VRF is used.
source {IPv4-ADDR IFNAME}	Specifies the source IPv4 address or interface to use.
do-not-fragment	Specifies the do-not-fragment (DF) bit in IP header of the Ping packet. This option does not allow the packet to be fragmented when it has to go through a segment with a smaller maximum transmission unit (MTU).

Examples

Pinging an IPv4 address:

```
switch# ping 10.0.0.0
PING 10.0.0.0 (10.0.0.0) 100(128) bytes of data.
108 bytes from 10.0.0.0: icmp_seq=1 ttl=64 time=0.035 ms
108 bytes from 10.0.0.0: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=3 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 10.0.0.0: icmp_seq=5 ttl=64 time=0.033 ms

--- 10.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.033/0.034/0.035/0.000 ms
```

Pinging the localhost:

```
switch# ping localhost
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.060 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.035 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.043 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.041 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.034 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.034/0.042/0.060/0.011 ms
```

Pinging a server with a data pattern:

```
switch# ping 10.0.0.2 data-fill 1234123412341234acde123456789012
PATTERN: 0x1234123412341234acde123456789012
PING 10.0.0.2 (10.0.0.2) 100(128) bytes of data.
108 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.207 ms
108 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.187 ms
108 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.225 ms
108 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.197 ms
108 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.210 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.187/0.205/0.225/0.015 ms
```

Pinging a server with a datagram size:

```
switch# ping 10.0.0.0 datagram-size 200
PING 10.0.0.0 (10.0.0.0) 200(228) bytes of data.
208 bytes from 10.0.0.0: icmp_seq=1 ttl=64 time=0.202 ms
208 bytes from 10.0.0.0: icmp_seq=2 ttl=64 time=0.194 ms
208 bytes from 10.0.0.0: icmp_seq=3 ttl=64 time=0.201 ms
208 bytes from 10.0.0.0: icmp_seq=4 ttl=64 time=0.200 ms
208 bytes from 10.0.0.0: icmp_seq=5 ttl=64 time=0.186 ms

--- 10.0.0.0 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.186/0.196/0.202/0.016 ms
```

Pinging a server with an interval specified:

```
switch# ping 9.0.0.2 interval 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.199 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.208 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.182 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.194 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 7999ms
rtt min/avg/max/mdev = 0.182/0.195/0.208/0.008 ms
```

Pinging a server with a specified number of packets to send:

```
switch# ping 9.0.0.2 repetitions 10
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.213 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.204 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.201 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.202 ms
108 bytes from 9.0.0.2: icmp_seq=6 ttl=64 time=0.184 ms
108 bytes from 9.0.0.2: icmp_seq=7 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=8 ttl=64 time=0.196 ms
108 bytes from 9.0.0.2: icmp_seq=9 ttl=64 time=0.193 ms
108 bytes from 9.0.0.2: icmp_seq=10 ttl=64 time=0.200 ms

--- 9.0.0.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8999ms
rtt min/avg/max/mdev = 0.184/0.197/0.213/0.008 ms
```

Pinging a server with a specified timeout:

```
switch# ping 9.0.0.2 timeout 3
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.175 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.192 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.190 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.181 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.197 ms

--- 9.0.0.2 ping statistics ---
```



```
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.175/0.187/0.197/0.007 ms
```

Pinging a server with the specified IP Type of Service:

```
switch# ping 9.0.0.2 tos 2
PING 9.0.0.2 (9.0.0.2) 100(128) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.033 ms
108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.031 ms
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.034 ms
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.031 ms

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.032/0.034/0.006 ms
```

Pinging a local host with the specified VRF.

```
switch# ping localhost vrf red
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.048 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.052 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.044 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.055 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.036/0.047/0.055/0.006 ms
```

Pinging the localhost with the default VRF:

```
switch# ping localhost vrf mgmt
PING localhost (127.0.0.1) 100(128) bytes of data.
108 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.085 ms
108 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.057 ms
108 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.047 ms
108 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.038 ms
108 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.059 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.038/0.057/0.085/0.016 ms
```

Pinging a server with the intermediate router time stamp:

```
switch# ping 9.0.0.2 ip-option include-timestamp
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.031 ms
TS:      59909005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.034 ms
```

```

TS:      59910005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.038 ms
TS:      59911005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.035 ms
TS:      59912005 absolute
        0
        0
        0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.037 ms
TS:      59913005 absolute
        0
        0
        0

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.031/0.035/0.038/0.002 ms

```

Pinging a server with the intermediate router time stamp and address:

```

switch# ping 9.0.0.2 ip-option include-timestamp-and-address
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.030 ms
TS:      9.0.0.2 60007355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.037 ms
TS:      9.0.0.2 60008355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.037 ms
TS:      9.0.0.2 60009355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.038 ms
TS:      9.0.0.2 60010355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.039 ms
TS:      9.0.0.2 60011355 absolute
        9.0.0.2 0
        9.0.0.2 0
        9.0.0.2 0

```

```

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.030/0.036/0.039/0.005 ms

```

Pinging a server with the intermediate router address:

```

switch# ping 9.0.0.2 ip-option record-route
PING 9.0.0.2 (9.0.0.2) 100(168) bytes of data.
108 bytes from 9.0.0.2: icmp_seq=1 ttl=64 time=0.034 ms
RR:      9.0.0.2
         9.0.0.2
         9.0.0.2
         9.0.0.2

108 bytes from 9.0.0.2: icmp_seq=2 ttl=64 time=0.038 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=3 ttl=64 time=0.036 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=4 ttl=64 time=0.037 ms (same route)
108 bytes from 9.0.0.2: icmp_seq=5 ttl=64 time=0.035 ms (same route)

--- 9.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.001 ms

```

Pinging a server with do-not-fragment:

```

switch# ping 192.168.1.8 datagram-size 2000 do-not-fragment
PING 192.168.1.8 (192.168.1.8) 2000(2028) bytes of data.
2008 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=0.721 ms
2008 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=0.792 ms
2008 bytes from 192.168.1.8: icmp_seq=3 ttl=64 time=0.857 ms
2008 bytes from 192.168.1.8: icmp_seq=4 ttl=64 time=0.833 ms
2008 bytes from 192.168.1.8: icmp_seq=5 ttl=64 time=0.836 ms

--- 192.168.1.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4056ms
rtt min/avg/max/mdev = 0.721/0.807/0.857/0.048 ms

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ping6

```
ping6 {<IPv6-ADDR> | <HOSTNAME>} [data-fill <PATTERN> | datagram-size <SIZE> |  
    interval <TIME> | repetitions <NUMBER> | timeout <TIME> | vrrp <VRID> |  
    vrf <VRF-NAME> | source <IPv6-ADDR> | <IFNAME>]
```

Description

Pings the specified IPv6 address or hostname with or without optional parameters. The VRRP option is provided to self-ping the configured link-local address on the VRRP group.

Parameter	Description
IPv6-ADDR	Selects the IPv6 address to ping.
HOSTNAME	Selects the hostname to ping. Range: 1-256 characters
data-fill <PATTERN>	Specifies the data pattern in hexadecimal digits to send. A maximum of 16 "pad" bytes can be specified to fill out the ICMP packet. Default: AB
datagram-size <SIZE>	Specifies the ping datagram size. Range: 0-65399, default: 100.
interval <TIME>	Specifies the interval between successive ping requests in seconds. Range: 1-60 seconds, default: 1 second.
repetitions <NUMBER>	Specifies the number of packets to send. Range: 1-10000 packets, default: Five packets.
timeout <TIME>	Specifies the ping timeout in seconds. Range: 1-60 seconds, default: 2 seconds.
vrrp <VRID>	Specifies the VRRP group ID.
vrf <VRF-NAME>	Specifies the virtual routing and forwarding (VRF) to use. When this option is not provided, the default VRF is used.
source <IPv6-ADDR> <IFNAME>	Specifies the source IPv6 address or interface to use.

Examples

Pinging an IPv6 address:

```
switch# ping6 2020::2  
PING 2020::2(2020::2) 100 data bytes  
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.386 ms  
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.235 ms  
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.249 ms  
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.240 ms  
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.252 ms  
  
--- 2020::2 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 0.235/0.272/0.386/0.059 ms
```

Pinging the localhost:

```

switch# ping6 localhost
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.093 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.051 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.055 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.046 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.048 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.046/0.058/0.093/0.019 ms

```

Pinging a server with a data pattern:

```

switch# ping6 2020::2 data-fill ab
PATTERN: 0xab
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.077 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.038/0.068/0.077/0.015 ms

```

Pinging a server with a datagram size:

```

switch# ping6 2020::2 datagram-size 200
PING 2020::2(2020::2) 200 data bytes
208 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.037 ms
208 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
208 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.077 ms
208 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.066 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.037/0.066/0.077/0.016 ms

```

Pinging a server with an interval specified:

```

switch# ping6 2020::2 interval 5
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.043 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.074 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.075 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.075 ms

--- 2020::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 19999ms
rtt min/avg/max/mdev = 0.043/0.068/0.075/0.014 ms

```

Pinging a server with a specified number of packets to send:

```

switch# ping6 2020::2 repetitions 6
PING 2020::2(2020::2) 100 data bytes
108 bytes from 2020::2: icmp_seq=1 ttl=64 time=0.039 ms
108 bytes from 2020::2: icmp_seq=2 ttl=64 time=0.070 ms
108 bytes from 2020::2: icmp_seq=3 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=4 ttl=64 time=0.076 ms
108 bytes from 2020::2: icmp_seq=5 ttl=64 time=0.071 ms
108 bytes from 2020::2: icmp_seq=6 ttl=64 time=0.078 ms

--- 2020::2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.039/0.068/0.078/0.015 ms

```

Pinging a local host with the specified VRF.

```

switch# ping6 localhost vrf red
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.050 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.039 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.027 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.027/0.038/0.050/0.010 ms

```

Pinging the localhost with the default VRF:

```

switch# ping6 localhost vrf mgmt
PING localhost(localhost) 100 data bytes
108 bytes from localhost: icmp_seq=1 ttl=64 time=0.032 ms
108 bytes from localhost: icmp_seq=2 ttl=64 time=0.022 ms
108 bytes from localhost: icmp_seq=3 ttl=64 time=0.040 ms
108 bytes from localhost: icmp_seq=4 ttl=64 time=0.022 ms
108 bytes from localhost: icmp_seq=5 ttl=64 time=0.046 ms

--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.022/0.032/0.046/0.010 ms

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

crypto pki application

```
crypto pki application <APP-NAME> certificate <CERT-NAME>
no crypto pki application <APP-NAME> certificate <CERT-NAME>
```

Description

Configures an application to associate with a user-configured certificate. By default, all applications are associated with the default certificate "local-cert".

Note that applications "captive-portal" and "hsc" are only available on certain platforms.

The certificate associated with EST client is global to all EST profiles.

Among the available applications, only dot1x-supplicant, est-client, and radsec-client are allowed to associate with device-identity certificate.

Also note that device-identity certificate on a switch using a TPM of legacy version 1.2 only works with TLS version 1.2.

1. When TLS min-version has been higher than 1.2, setting application with device-identity from CLI on a TPM 1.2 switch will be rejected; setting such configuration through REST will make the certificate association invalid and local-cert will be used for the affected application instead.
2. On a TPM 1.2 switch with TLS min-version 1.2 and with a client application associated with device-identity certificate, the client will be limited to sha256WithRSA, sha384WithRSA, and sha512WithRSA for signature algorithms. Given that limit, the underlying crypto library may remove the cipher suites involving ECDSA from the client side offering at runtime even if such cipher suites are allowed in user configuration.

Note that if user makes such conflicting configuration through REST, it cannot be rejected by CLI. Instead, certificate manager will be able to detect the situation, set the application association with device-identity certificate as invalid, force the application to use local-cert, and log an event like this:

```
2025-03-10T22:55:01.525478+00:00 8320 certmgr[2465]: Event|7724|LOG_ERR|AMM|1/1|
```

The device-identity certificate of this system is only compatible with TLS 1.2, but the configured TLS min-version is higher or no TLS 1.2 cipher-suite is configured. Associated applications will use local-cert instead.

The **no** form of this command associates the specified feature with the default certificate.

Parameter	Description
<APP-NAME>	Specifies the name of a feature on the switch: ▪ captive-portal: Captive portal ▪ est-client: EST client

Parameter	Description
	▪ hsc: Hardware switch controller ▪ https-server: HTTPS server ▪ radsec-client: RadSec client ▪ syslog-client: Syslog client syslog-client communicates with syslog server over TLS. You can associate a certificate with the syslog-client application by enrolling the certificate manually or through EST.
<code><CERT-NAME></code>	Specifies the name of an installed leaf certificate.

Examples

Associating the EST client with leaf certificate **leaf-cert1**:

```
switch(config)# crypto pki application est-client certificate leaf-cert1
```

Associating the syslog client with leaf certificate **leaf-cert**:

```
switch(config)# crypto pki application syslog-client certificate leaf-cert
```

Setting the syslog client to use the default certificate:

```
switch(config)# no crypto pki application syslog-client certificate
```

Setting the RadSec client to use the default certificate:

```
switch(config)# no crypto pki application radsec-client certificate
```

Associating the RadSec client with leaf certificate **leaf-cert**:

```
switch(config)# crypto pki application radsec-client certificate leaf-cert
```

Associating the HTTPS server with leaf certificate **leaf-cert2**:

```
switch(config)# crypto pki application https-server certificate leaf-cert2
```

Associating the 802.1X supplicant with leaf certificate **cert1**:

```
switch(config)# crypto pki application dot1x-suppliant certificate cert1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

crypto pki certificate

```
crypto pki certificate <CERT-NAME>
no crypto pki certificate <CERT-NAME>
```

Description

Creates a leaf certificate and changes to its context **config-cert-<CERT-NAME>**. If the specified leaf certificate exists, this command changes to its context.

The first time the switch starts it creates a self-signed, default leaf certificate called **local-cert**. This certificate is used by any switch application that does not have an associated leaf certificate.

The **no** form of this command deletes the specified leaf certificate. The default leaf certificate **local-cert** cannot be deleted.

Parameter	Description
<CERT-NAME>	Specifies the name of a leaf certificate. Range: 1 to 32 alphanumeric characters (excluding ").

Examples

Creating leaf certificate **leaf-cert**:

```
switch(config)# crypto pki certificate leaf-cert
switch(config-cert-leaf-cert)#
```

Deleting leaf certificate **leaf-cert**:

```
switch(config)# no crypto pki certificate leaf-cert
The leaf certificate has associated applications. Deleting the certificate
will make the applications use the default certificate local-cert.
Continue (y/n)? y
switch(config)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

crypto pki ta-profile

```
crypto pki ta-profile <TA-NAME>
no crypto pki ta-profile <TA-NAME>
```

Description

Creates a trust anchor (TA) profile and changes to the **config-ta-<TA-NAME>** context for the profile. Each TA profile stores the certificate for a trusted CA. Up to 64 profiles can be defined.

If the specified TA profile exists, this command changes to the **config-ta-<TA-NAME>** context for the profile.

The **no** form of this command removes the specified TA profile.



When creating a new profile, If you exit the **config-ta-<TA-NAME>** context without importing the TA certificate, the profile is discarded.

Parameter	Description
<TA-NAME>	Specifies the TA profile name. Range: 1 to 48 alphanumeric characters excluding ". NOTE: The TA profile name cannot end with est-ta<nn> where <nn> is 00 to 99 . For example, company-trust-anchor-est-ta01 is not allowed. This TA profile name suffix is reserved for TA profiles that are created for CA certificates from EST servers.

Examples

Creating the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)#
```

Removing TA profile **root-cert**:

```
switch(config)# no crypto pki ta-profile root-cert
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

enroll self-signed

enroll self-signed

Description

Generates a key pair and generates a self-signed certificate with it.

The subject fields and key type of the current leaf certificate must be defined before running this command. If not, you are prompted to fill in the subject fields, and the key type is set to **RSA 2048**.

Example

Enrolling the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# enroll self-signed
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Rocklin, OU=Site, O=Comp,
        CN=Leaf01
Key Type: RSA (2048)

Continue (y/n)? y
Self-signed certificate is created and enrolled successfully.

switch(config-cert-leaf-cert)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert- <i><CERT-NAME></i>	Administrators or local user group members with execution rights for this command.

enroll terminal

enroll terminal

Description

Generates a key pair and certificate signing request (CSR) for the current leaf certificate. Use the CSR to obtain a signed certificate from a certificate authority (CA), and then import the certificate onto the switch with the command **import terminal**.

The key type, and the certificate common name in the subject fields of the current leaf certificate must be completed before running this command. After this command is issued, any configuration change in the same certificate context will not be reflected in the generated CSR or certificate until you issue an **enroll** command again.

Usage

The subject fields and/or subject alternative name are usually already configured before the **enroll terminal** command is issued. If both subject fields and subject alternative name are not preconfigured, the command-line interface will prompt the user to confirm, using the serial number as subject common name. If subject alternative name is preconfigured but all subject fields are not, the command-line interface will prompt the user to confirm making the subject alternative name a critical extension (as per RFC 5280 Section 4.1.2.6). If the subject common name is preconfigured but all other subject fields are empty, it is considered the user's decision to leave them empty.

In auto-confirm and CLI config downloads, if both subject alternative name and subject common name are not pre-configured, the switch will automatically use serial number as subject common name and use other subject fields as is, including being empty. If the subject alternative name is preconfigured and all subject fields are not, the switch will automatically make subject alternative name a critical extension for certificate enrollment.

Note that although RFC 5280 allows leaving subject fields all empty when a subject alternative name is present and marked as critical, many servers and applications do not tolerate this. *It is strongly recommended to populate at least the common name of the subject even if the subject alternative name is present.*

Example

```
switch(config-cert-8400-1)# enroll terminal
You are enrolling a certificate with the following attributes:
Subject: C=US, ST=CA, L=Roseville, OU=Aruba-Roseville, O=Aruba, CN=8400-1
Key Type: RSA (2048)
Key Usage: nonRepudiation
Ext Key Usage: clientAuth, codeSigning
Subject Alternative Name: DNS:example1.com, IP:1.1.1.1, IP:2222::2222

Continue (y/n)? y
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Comand introduced.

Command Information

Platforms	Command context	Authority
All platforms	<code>config-cert-<CERT-NAME></code>	Administrators or local user group members with execution rights for this command.

ext-key-usage

`[no] ext-key-usage {server-auth | client-auth}`

Description

Configure extended-key-usage extensions for certificate enrollment.

The **no** form of this command negates or removes any configuration parameter.

Parameter	Description
<code>client-auth</code>	Configure use of key for client authentication
<code>server-auth</code>	Configure use of key for server authentication

Usage

Extended-key-usage options are specified in [RFC 5280](#). AOS-CX switches support the configuration of the **id-kp-serverAuth** and **id-kp-clientAuth** options described in this RFC.

Setting multiple key-usage options for a certificate:

```
switch(config)# crypto pki certificate leaf-cert
switch (config-cert-leaf-cert)# ext-key-usage client-auth
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# ext-key-usage server-auth
switch (config-cert-leaf-cert)#
```

Removing an option from a extended-key-usage extension for the certificate to be enrolled.

```
switch(config)# crypto pki certificate leaf-cert
switch (config-cert-leaf-cert)# no ext-key-usage client-auth
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# no ext-key-usage server-auth
switch (config-cert-leaf-cert)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Comand introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

import (CA-signed leaf certificate)

```
import terminal ta-profile <TA-NAME> [password <PW>]
import <REMOTE-URL> ta-profile <TA-NAME> [password <PW>] [vrf <VRF-NAME>]
import <STORAGE-URL> ta-profile <TA-NAME> [password <PW>]
```

Description

Imports a CA-signed leaf certificate and then validates the certificate against the specified TA profile. If the imported data includes a private key, the private key must match the leaf certificate being imported. If the imported data does not include a private key, the certificate must match a CSR that was previously generated with the command **enroll terminal** and must be signed by the CA whose root certificate is installed in the specified TA profile. The TA profile must exist and have a TA certificate configured.

Parameter	Description
terminal	Import the certificate by pasting PEM-format data at the console. Upon execution, the config-cert-import context is entered for certificate pasting. To complete certificate data entry press Control-D in your terminal program. Alternatively, the pasted certificate data can include at its end the delimiter END_OF_CERTIFICATE (after the -----END CERTIFICATE----- line), making entry of Control-D unnecessary.
ta-profile <TA-NAME>	Specifies the TA profile name. Range: 1 to 48 alphanumeric characters excluding ".
password <PW>	Specifies the plaintext password used to decrypt the private key in the imported certificate data. When this parameter is omitted, the password is prompted for as required. Range: 1 to 32 alphanumeric characters.
<REMOTE-URL>	Specifies a certificate data file on a remote TFTP or SFTP server. The URL syntax is: {tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE>
vrf <VRF-NAME>	Specifies the name of the VRF to use for the remote URL file transfer. The default is mgmt .
<STORAGE-URL>	Available on switch families that provide USB device file import capability, specifies a certificate data file on a USB storage device inserted in the switch USB port. The URL syntax is usb:/<FILE> .

Usage

- The imported data must include all the intermediate CA certificates in the certificate chain leading to the certificate imported into the specified TA profile.
- This command cannot be used with the default certificate **local-cert**.
- The PEM data format is supported for all import sources. The PKCS#12 data format is supported for **<REMOTE-URL>** and **<STORAGE-URL>**.
- The PEM data must be delimited with these lines for the certificate data:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

And the PEM data must be delimited with either of these line pairs for the private key data:

```
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
```

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
-----END ENCRYPTED PRIVATE KEY-----
```

Examples

Importing a leaf certificate from the console:

```
switch(config)# crypto pki certificate leaf-cert
switch(config-cert-leaf-cert1)# import terminal ta-profile root-cert
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIIFRDCCAyygAwIBAgQP8nS2Vp15u0xXMdkDJzANBgkqhkiG9w0Bv
switch(config-cert-import)# MQswCQYDVQGEwJVUEOMAwGA1UCgwFXJ1YmDAGNBAMM1Jvb3QgQ0Ew
switch(config-cert-import)# HhcNMTkNDEwMjIwNTI1WhcjIwMTOMjwNE1WjzQswQDVQGEwJVUzEL
...
switch(config-cert-import)# 1fIYZYGQyla0AwFuPTTxBXHYWRxTPbUYU5umJfRPmE4VY8S9DQgcr
switch(config-cert-import)# 1NGNm3NG03GqPScs/TF9bVyFA5BOS5lmmkfRYK8D/kMTfRreSdxis
switch(config-cert-import)# YQ1u1NqShps=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9wBBQ0wMzAbBgqkw0QwwDQIpJMN7sVGwCAggA
switch(config-cert-import)# MBQGCCqGSib3DQMHAit+2qadNAASCgLYJ4Am3EfhH5p51Ggr86VqS
switch(config-cert-import)# IJ6L/UhEtH523nUkdV6gvAgoYaD83PswToAGv5VS8OMFTPttrn5/K
...
switch(config-cert-import)# OgSecqZsG6arbx0ESaYBir1c/6rPspcjbX283iD1MWOpes2aEmOX
switch(config-cert-import)# iKnXnUMpVPfLc74ty2S41DtH0X9gf6aa1jStg+7cND9XfGtjaV2+/
switch(config-cert-import)# cb4=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated with root-cert and imported successfully.
switch(config-cert-leaf-cert)#
```

Importing a leaf certificate from a remote file:

```
switch(config)# crypto pki certificate leaf-cert2
switch(config-cert-leaf-cert2)# import tftp://1.1.1.2/c2.p12 ta-profile root-cert
% Total      % Received % Xferd  Average Speed   Time    Time       Time    Current
           Dload    Upload   Total   Spent    Left     Speed
100 3722 100 3722    0     0 391k      0  --:--:-- --:--:-- --:--:-- 391k
100 3722 100 3722    0     0 376k      0  --:--:-- --:--:-- --:--:-- 376k
Enter import password: *****
Leaf certificate is validated with root-cert and imported successfully.
switch(config-cert-leaf-cert2)#
```




For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert- <i><CERT-NAME></i>	Administrators or local user group members with execution rights for this command.

import (self-signed leaf certificate)

```
import terminal self-signed [password <PW>]
import <REMOTE-URL> self-signed [password <PW>] [vrf <VRF-NAME>]
import <STORAGE-URL> self-signed [password <PW>]
```

Description

Imports a self-signed leaf certificate including its matching private key.

Parameter	Description
terminal	Import the certificate by pasting PEM-format data at the console. Upon execution, the config-cert-import context is entered for certificate pasting. To complete certificate data entry press Control-D in your terminal program. Alternatively, the pasted certificate data can include at its end the delimiter END_OF_CERTIFICATE (after the -----END CERTIFICATE----- line), making entry of Control-D unnecessary.
password <PW>	Specifies the plaintext password used to decrypt the private key in the imported certificate data. When this parameter is omitted, the password is prompted for as required. Range: 1 to 32 alphanumeric characters.
<REMOTE-URL>	Specifies a certificate data file on a remote TFTP or SFTP server. The URL syntax is: {tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE>
vrf <VRF-NAME>	Specifies the name of the VRF to use for the remote URL file transfer. The default is mgmt .
<STORAGE-URL>	Available on switch families that provide USB device file import capability, specifies a certificate data file on a USB storage device inserted in the switch USB port. The URL syntax is usb:/<FILE> .

Usage

- This command cannot be used with the default certificate **local-cert**.
- The PEM data format is supported for all import sources. The PKCS#12 data format is supported for **<REMOTE-URL>** and **<STORAGE-URL>**.
- The PEM data must be delimited with these lines for the certificate data:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

And the PEM data must be delimited with either of these line pairs for the private key data:

```
-----BEGIN PRIVATE KEY-----
-----END PRIVATE KEY-----
```

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
-----END ENCRYPTED PRIVATE KEY-----
```

Example

Importing a self-signed leaf certificate from the console:

```
switch(config)# crypto pki certificate ss-leaf-cert
switch(config-cert-ss-leaf-cert)# import terminal self-signed
Paste the certificate in PEM format below, then hit enter and ctrl-D:
switch(config-cert-import)# -----BEGIN CERTIFICATE-----
switch(config-cert-import)# MIID2TCCAsGgAwIBAgIJAKcrqokm6p9GMA0GCSqGSIb3DQEBCwUAM
switch(config-cert-import)# tDCCA5ygAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwwGgAwCzABAYTA1
switch(config-cert-import)# VQQGEwJVZUzELMAkGA1UECAwCQ0ExDTALBgNVBACMBFJvc2UxDDAKB
...
switch(config-cert-import)# +fWQLxhp+jKJGZGOZz/FENt2uSfZHxlXiu8n3g+EgqExenYlpBRJr
switch(config-cert-import)# VuEEoNb/YfkPXXHva4Zfx223q+f694wlVsHkENSzqr2goHpa2fOzq
switch(config-cert-import)# alewddmVqCES+x8bvfh3C/6IB6ePkEsnMlHNTeM=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)# MIIFDjBABGkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIT8Ni3
switch(config-cert-import)# MBQGCCqGSIb3DQMHBAiBHrejkdpcdASCBMjVxrrYYPNt3V1abr9k8
switch(config-cert-import)# 5GE0U99awh9ys4360WR95xOFGThvjKTyRWG511nGwVeLZs/7TPXWI
...
switch(config-cert-import)# hzc5ZT/w2F08icRI5mFbGoTAAw9IIWMOXGweaWQJdYKGrhg89GrnV
switch(config-cert-import)# M2UuP/tYuu0328QcenKZEJmZKCbx78oFRR+pgma4oeMaFTIyXE6Pr
switch(config-cert-import)# GAdCK8tkDiJ9DKbqdm5W0/nTJfqwUQlfl127dNrBAodsHdwr3UR99H
switch(config-cert-import)# SPo=
switch(config-cert-import)# -----END ENCRYPTED PRIVATE KEY-----
switch(config-cert-import)#
Enter import password: *****
Leaf certificate is validated as self-signed certificate and imported
successfully.
switch(config-cert-ss-leaf-cert)#
```

Importing a leaf certificate from a remote file:

```
switch(config)# crypto pki certificate ss-leaf-cert2
switch(config-cert-ss-leaf-cert2)# import tftp://1.1.1.2/ss2.p12 self-signed
  % Total      % Received % Xferd  Average Speed   Time    Time       Time    Current
                               Dload  Upload    Total     Spent    Left     Speed
100  3230  100  3230    0     0   875k      0  --:--:-- --:--:-- --:--:--   875k
100  3230  100  3230    0     0   831k      0  --:--:-- --:--:-- --:--:--   831k
Enter import password: *****
Leaf certificate is validated as self-signed certificate and imported
successfully.
switch(config-cert-ss-leaf-cert2)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

key-type

```
key-type {rsa [key-size <K-SIZE>] | ecdsa [curve-size <C-SIZE>]}
```

Description

Sets the key type and key size for the current leaf certificate. The key type of the default certificate **local-cert** cannot be changed.

Parameter	Description
rsa	Selects the RSA key type.
key-size <K-SIZE>	Specifies the RSA key size in bits. Supported values: 2048, 3072, 4096. Default: 2048
ecdsa	Selects the ECDSA key type.
curve-size <C-SIZE>	Specifies the ECDSA elliptic curve size in bits. Supported values: 256, 348, 521. Default: 256

Examples

Setting RSA encryption on the leaf certificate **leaf-cert**:

```
switch(config)# crypto pki certificate leaf-cert  
switch(config-cert-leaf-cert)# key-type rsa key-size 3072
```

Setting ECDSA encryption on the leaf certificate **leaf-cert**:

```
switch(config)# crypto pki certificate leaf-cert  
switch(config-cert-leaf-cert)# key-type ecdsa curve-size 521
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-cert-<CERT-NAME></code>	Administrators or local user group members with execution rights for this command.

key-usage

```
{no} key-usage
    data-encipherment
    digital-signature
    key-encipherment
    key-agreement
    key-restriction {encipher-only | decipher-only}
    non-repudiation
```

Description

Configure key-usage extensions for certificate enrollment. Users can select zero, one, or multiple key usage options. The selected options will be set into the key-usage extension field of the CSR for the certificate. The CA server that signs the certificate determines whether or not to grant the options, and which option(s) to grant. As a result, after the certificate is successfully enrolled, the key-usage extension field may appear differently from the original user configuration.

The **no** form of this command negates or removes any configuration parameter.

Parameter	Description
<code>data-encipherment</code>	Configure use of key for encrypting data
<code>digital-signature</code>	Configure use of key for digital signature validation
<code>key-encipherment</code>	Configure use of key for encrypting keys
<code>key-agreement</code>	Configure use of key for key exchange between parties
<code>key-restriction {encipher-only decipher-only}</code>	Configure restriction of key on key-agreement usage with one the following options: ▪ decipher-only: Configure restriction of key as decipher only ▪ encipher-only: Configure restriction of key as encipher only
<code>non-repudiation</code>	Configure use of key for non-repudiation service

Examples

Setting multiple key-usage options for a certificate:

```

switch(config)# crypto pki certificate leaf-cert
switch (config-cert-leaf-cert)# key-usage digital-signature
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# key-usage non-repudiation
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# key-usage key-restriction encipher-only
Encipher-only and decipher-only options will not take effect until key-agreement
option
is enabled.
Continue (y/n)? y
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# key-usage key-agreement
switch (config-cert-leaf-cert)#

```

Removing an option from a key-usage extension for the certificate to be enrolled

```

switch (config-cert-leaf-cert)# no key-usage digital-signature
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# no key-usage non-repudiation
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# no key-usage key-agreement
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# no key-usage key-restriction
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# no key-usage key-restriction encipher-only
switch (config-cert-leaf-cert)#

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Comand introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

ocsp disable-nonce

```

ocsp disable-nonce
no ocsp disable-nonce

```

Description

Configures exclusion of the nonce from OCSF requests. A nonce is a unique identifier that an OCSF client inserts in an OCSF request and expects the OCSF responder to include it in the corresponding OCSF response. The nonce mechanism helps prevent replay attacks in which a malicious player attempts to masquerade as the OCSF responder. Although the nonce is included by default, it can be

excluded. Some OCSP responders choose to not support the use of the nonce due to performance considerations.

The **no** form of this command re-enables nonce inclusion in OCSP requests.

Examples

Disable inclusion of the nonce in OCSP requests for TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# ocsp disable-nonce
```

Enable inclusion of the nonce in OCSP requests for TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# no ocsp disable-nonce
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta-<TA-NAME>	Administrators or local user group members with execution rights for this command.

ocsp enforcement-level

```
ocsp enforcement-level {strict | optional}  
no enforcement-level
```

Description

Sets either strict or reduced enforcement of the OCSP check of certificates. Strict enforcement is enabled by default.

The **no** form of this command resets enforcement to its default of **strict**.

Parameter	Description
strict	Sets strict OCSP checking of certificates. The certificate is accepted only if all possible checking (including validation failures, software system errors, configuration errors, transactional errors) is successful.
optional	Sets reduced OCSP checking of certificates. The certificate is

Parameter	Description
	accepted unless one or more of these validation errors occur: ▪ Response signature invalid. ▪ Nonce in response mismatch. ▪ Certificate revoked, but only when revocation checking is possible. if revocation check is not possible, the certificate is still accepted if there are no other validation errors.

Examples

Setting reduced OCSP checking of certificates:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# ocsf enforcement-level optional
```

Setting strict OCSP checking of certificates:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# ocsf enforcement-level strict
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta- <i><TA-NAME></i>	Administrators or local user group members with execution rights for this command.

ocsp url

```
ocsp url {primary | secondary} <URL>
no ocsp url {primary | secondary}
```

Description

Configures the OCSP responder URLs that the current TA profile uses to verify the revocation status of an X.509 digital certificate. These URLs override the OCSP responder URL contained within the peer certificate being verified (as well as URLs defined in any intermediate CAs in the chain of trust).

If no OCSP responder URLs are defined for a TA profile (default setting), then the OCSP responder URL in the peer certificate is used for revocation status checking. (The OCSP responder URL is contained in a certificate's Authority Information Access field, which is an X.509 v3 certificate extension.)

The **no** form of this command deletes the specified OCSP responder URL (primary or secondary) from the current TA profile.

Parameter	Description
{primary secondary} <URL>	Specify the HTTP URL of the primary or secondary OCSP responder using either a fully qualified domain name or IPv4 address.

Examples

Defining the primary OCSP URL for the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# revocation-check ocsp  
switch(config-ta-root-cert)# ocsp url primary http://ocsp-server.site.com
```

Removing the primary OCSP URL from the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile oot-cert  
switch(config-ta-root-cert)# revocation-check ocsp  
switch(config-ta-root-cert)# no ocsp url primary
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta-<TA-NAME>	Administrators or local user group members with execution rights for this command.

ocsp vrf

```
ocsp vrf <VRF-NAME>  
no ocsp vrf
```

Description

Sets the VRF that the switch uses to communicate with OCSP responders for OCSP checking. VRF mgmt is used by default.

The **no** form of this command resets the VRF to its default **mgmt**.

Parameter	Description
<VRF-NAME>	Specifies the name of the VRF the switch uses to communicate with OSCP responders. Default: mgmt .

Examples

Setting the OSCP responder VRF to **corp1**:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# oosp vrf corp1
```

Reverting the OSCP responder VRF to its default:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# no oosp vrf
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta-<TA-NAME>	Administrators or local user group members with execution rights for this command.

revocation-check oosp

```
revocation-check oosp
no revocation-check
```

Description

Enables certificate revocation checking for the current profile using the online certificate status protocol (OCSP).

The **no** form of this command disables certificate revocation checking for the current profile.

Examples

Enabling revocation checking for the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# revocation-check oosp
```

Disabling revocation checking for the TA profile **root-cert**:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# no revocation-check
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-ta-<TA-NAME>	Administrators or local user group members with execution rights for this command.

show crypto pki application

```
show crypto pki application
```

Description

Shows certificate information for all features (applications) using leaf certificates that are managed by PKI.

Examples

Showing certificate information for all features (applications) using leaf certificates:

```
switch# show crypto pki application1
```

Associated Applications	Certificate Name	Cert Status
https-server		not configured, using local-cert
syslog-client	local-cert	valid
hsc	xhscert	invalid, using local-cert
radsec-client	device-identity	valid



For more information on features that use this command, refer to the Security Guide for your switch model.

Security Considerations

1. When creating the Certificate Configuration:

- Replace the default `local-cert` with CA-signed certificates
- Include IP addresses and hostnames in Subject Alternative Names (SANs)
- Ensure certificate validity periods and renewal processes

2. When configuring gNMI clients (external to CX devices):

- Avoid using client options which bypass security checks in production environments.

These are typically used to speed up the integration process but should not be permanent.

- For example, the `--skip-verify` flag on the `gnmic` client or `-insecure` on the `grpcurl` client.
- Configure clients with proper CA certificate stores
- Implement certificate pinning where supported

3. For the Network Architecture:

- Deploy gNMI on dedicated management VRFs
- Use network segmentation to isolate gNMI traffic
- Consider additional network-level security controls

Risk Mitigation

Given the case a certificate validation bypass must be used temporarily follow these suggestions:

- Document the security risk in change management
- Limit usage to isolated lab/test environments
- Implement compensating network security controls
- Plan migration to proper certificate validation

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show crypto pki certificate

```
show crypto pki certificate [<CERT-NAME> [plaintext | pem]]
```

Description

Shows a list of all configured leaf certificates, or detailed information for a specific leaf certificate.

Possible values for Cert Status are: **CSR pending, expired, expires soon, installed, malformed, not yet known.**

Possible values for EST Status are: **enroll failed, enroll pending, enroll retrying, enroll success, n/a** (certificate is not EST-enrolled), **reenroll failed, reenroll pending, reenroll retrying.**

Parameter	Description
<CERT-NAME>	Specifies the leaf certificate name. Range: 1 to 32 alphanumeric characters excluding ".".
plaintext	Shows certificate information in plain text.
pem	Shows certificate information in PEM format.

Examples

Showing a list of all configured leaf certificates:

```
switch# show crypto pki certificate
```

Certificate Name	Cert Status	EST Status	Associated Applications
local-cert	installed	n/a	radsec-client, captive-portal
device-identity	installed	n/a	none
pod01-99-1	installed	n/a	https-server, est-client
syslog-1	CSR pending	enroll retrying	syslog-client
leaf-cert1	installed	enroll success	none
leaf-cert2	CSR pending	enroll failed	none

Showing detailed information (in plaintext format) for leaf certificate **pod01-99-1**:

```
switch# show crypto pki certificate pod01-99-1 plaintext
```

```
Certificate Name: pod01-99-1
Associated Applications:
  https-server, est-client
Certificate Status: installed
EST Status: n/a
Certificate Type: regular
Intermediates:
  Subject: C = US, ST = CA, O = Company, OU = Lab-IT, CN = DeviceCA
  Issuer: C = US, ST = CA, O = Company, OU = Lab-IT, CN = Lab-CA
  Serial Number: 0x02
  Subject: C = US, ST = CA, O = Company, OU = Lab-IT, CN = Lab-CA
  Issuer: C = US, ST = CA, O = Company, OU = Lab-IT, CN = Lab-Root
  Serial Number: 0x01
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 14529416756121781768 (0xc9a2db8f3e3f4608)
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=US, ST=CA, OU=Lab-IT, O=Company, CN=DeviceCA
  Validity
    Not Before: Jan 12 23:36:57 2018 GMT
    Not After : Nov 1 23:36:57 2020 GMT
  Subject: C=US, ST=CA, OU=Lab-IT, O=Company, CN=pod01-99-1
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:a0:cd:ef:1b:f9:b8:bd:39:fc:7a:0e:00:17:ff:
      2b:72:d8:4e:d4:df:49:36:ca:3a:f9:05:05:d7:e3:
      d1:97:29:71:e6:33:b8:bb:8e:f0:ee:a6:e4:4a:f8:
      ...
      fe:dd:d9:a0:af:59:47:25:b4:34:06:af:03:1d:33:
      30:c3:85:fe:5c:e7:19:7f:ff:3a:b2:21:b8:e8:ed:
      83:09
    Exponent: 65537 (0x10001)
  Signature Algorithm: sha256WithRSAEncryption
    39:f6:03:86:03:d9:05:61:39:25:5f:0d:75:cc:05:ae:04:7e:
    4c:a3:13:0b:f0:1e:af:68:0e:40:9f:ed:48:b6:5e:56:8c:53:
    46:5b:c9:a4:e0:b0:bc:31:4b:a7:5d:0a:ed:7c:9c:f6:bf:1e:
```

```
...
39:f5:26:58:68:e2:13:ec:94:ac:60:8e:4b:b0:ba:45:cf:d6:
6a:4b:9f:7d:ae:3f:e5:2e:81:fe:ac:b3:65:44:35:47:a5:2f:
89:e7:58:a0
```

Showing detailed information (in PEM format) for leaf certificate **leaf-cert1** with a status of **CSR pending**:

```
switch# show crypto pki certificate leaf-cert1 pem

Certificate Name: leaf-cert1

Associated Applications:
  syslog-client
Certificate Status: CSR pending
EST Status: enroll retrying
Certificate Type: regular
-----BEGIN CERTIFICATE REQUEST-----

MIICtTCCAzoCAQAwcDEWMBQGA1UEAxMNC3lzbG9nLTg0MBYGA1UECxMPQ
XJlYmEtUm9zZXZpbGxlMQ4wDAYDVQQKEYTESMBAGA1EBxMJU9zZXZpbG
xlMQswCQYDVQQIEWJDQTELMAGA1UEBhMCVVMwggeiMSIb3DQEBAQUAA4I
...
cw2ytN6Idgh8lk59x6DH7V/eORaKd5lq+oO7nkr6+QBf5L3f5Kb+TOFio
lei+EdCHMxxc07MK0n3dkziSW25HFUGsyEXVMK+BID3zbKDoUe6XVhvqI
mamXyghigLYDcbSn6WVw==
-----END CERTIFICATE REQUEST-----
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show crypto pki ta-profile

```
show crypto pki ta-profile [<TA-NAME>]
```

Description

Shows a list of all configured TA profiles, or detailed information for a specific profile.



This command shows information for both directly-configured TA profiles and TA profiles that were dynamically downloaded from EST servers.

Parameter	Description
<TA-NAME>	Specifies the TA profile name. Range: 1 to 48 alphanumeric characters excluding ".".

Examples

Showing a list of all configured TA profiles:

```
switch# show crypto pki ta-profile
```

Profile Name	TA Certificate	Revocation Check
BASE_CA	Installed,valid	disabled
BASE02_CA	Installed,expired	disabled
root-cert	Installed,valid	OCSP
ROOT-A_CA	Not Installed	OCSP
EST-Service1	Installed,valid	None
EST-Service2	Installed,valid	None

Showing detailed information for TA profile **root-cert**:

```
switch# show crypto pki ta-profile root-cert
```

```
TA Profile Name       : root-cert
Revocation Check      : OCSP
  OSCP Primary URL    : http://ocsp1.domain.com
  OSCP Secondary URL  : Not Configured
  OSCP Disable-nonce  : false
  OSCP Enforcement Level: strict
  OSCP VRF            : mgmt
TA Certificate: Installed and valid
Version: 3 (0x2)
Serial Number:
  74:e6:6d:22:3f:52:cc:94:43:41:ab:66:a8:8d:47:b1
Signature Algorithm: sha1withRSAEncryption
Issuer: OU=DeviceTrust, OU=Operations, O=Site, C=US,
       CN=Site Trusted Computing Root CA 1.0
Validity
  Not Before: Sep 14 03:12:06 2007 GMT
  Not After : Sep 14 03:21:14 2032 GMT
Subject: OU=DeviceTrust, OU=Operations, O=Site, C=US,
       CN=Site Trusted Computing Root CA 1.0
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (2048 bit)
  Modulus (2048 bit):
    30:0d:06:09:2a:86:48:86:f7:0d:01:01:01:05:33:
    03:82:01:0f:00:30:82:01:3a:02:82:01:01:00:ac:
    3d:60:3a:2e:ca:a4:34:db:5c:3b:6b:07:df:73:62:
    ...
    20:c8:df:63:14:5a:e8:d3:ea:83:d8:47:a3:b5:2e:
    bb:64:51:f0:be:13:b6:91:e4:32:45:58:5e:1f:0d:
    02:03:01:00:01
  Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage:
    Digital Signature, Certificate Signing, CRL Signing
  X509v3 Basic Constraints:
```

```
CA:TRUE, pathlen:4
X509v3 Subject Key Identifier:
    eb:d7:ec:db:8a:cb:f2:51:d5:06:e1:42:7b:39:a7:d0:1e:31:6e:bf

Signature Algorithm: sha1withRSAEncryption
    1c:90:f3:a4:f0:0d:e2:e3:e9:ae:01:e1:7d:a7:13:e2:cc:0b:
    17:31:26:92:a2:5d:1d:19:60:54:03:13:9b:e1:73:6c:e4:b3:
    01:4f:4e:ae:61:bd:ae:b6:12:d3:ab:08:ae:8c:47:92:d7:0d:
    ...
    ca:cf:11:78:55:6d:06:49:fa:d4:8d:f3:ef:7f:79:38:35:5d:
    16:5a:57:7f:a8:dc:b0:f8:a2:04:0d:17:0b:bb:58:32:30:e0:
    2d:a8:37:a2
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

subject

```
subject [common-name <COMMON-NAME>] [country <COUNTRY>] [locality <LOCALITY>]
        [org <ORG-NAME>] [org-unit <ORG-UNIT>] [state <STATE>]
```

Description

Sets the subject fields for the current leaf certificate. If the **common-name** parameter is not specified, then you are prompted to define a value for each field. If a configured value exists for any field, it is presented as the default.

The subject fields of the default certificate **local-cert** cannot be changed.

Parameter	Description
<code>common-name <COMMON-NAME></code>	Specifies the common name. The name can be a single word or multiple words enclosed in quotation marks (").
<code>country <COUNTRY></code>	Specifies the country or region using the two letter ISO 3166-1 country code.
<code>locality <LOCALITY></code>	Specifies the locality such as city or region. The locality can be a single word or multiple words enclosed in quotation marks (").
<code>org <ORG-NAME></code>	Specifies the organization. The org name can be a single word or multiple words enclosed in quotation marks (").

Parameter	Description
<code>org-unit <ORG-UNIT></code>	Specifies the organizational unit (OU). The OU can be a single word or multiple words enclosed in quotation marks ("). Define multiple OUs by separating the names with commas (,).
<code>state <STATE></code>	Specifies the state. The state can be a single word or multiple words enclosed in quotation marks (").

Examples

Setting subject fields for the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# subject common-name Leaf01 country US
locality Roseville org "HPE Aruba" org-unit Storage,Server state CA
```

Setting subject fields for the leaf certificate **leaf-cert** interactively:

```
switch(config-cert-leaf-cert)# subject
Do you want to use the switch serial number as the common name (y/n)? n
Enter Common Name : Leaf01
Enter Org Unit : Storage,Server
Enter Org Name : HPE Aruba
Enter Locality : Roseville
Enter State : CA
Enter Country : US
switch(config-cert-leaf-cert)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-cert-<CERT-NAME></code>	Administrators or local user group members with execution rights for this command.

subject-alt-name

[no] subject-alt-name {dns-name <dns-name> | ip <ip-address>}

Description

Configure subject alternative name (SAN) extensions for certificate enrollment. SAN extensions are specified in [RFC 5280](#). The switch supports both **dnsName** and **ipAddress** types, with a maximum of two entries for each type.

The **no** form of this command negates or removes any configuration parameter.

Parameter	Description
dns-name <dns-name>	Configure a SAN entry containing a DNS name. The DNS name can contain no more than 255 characters.
ip <ip-address>	Configure a SAN entry containing an IP address in either IPv4 or IPv6 format.

Usage

For more information on using this configuring a subject Alternative name during CSR creation, refer to the [video on the HPE Aruba Networking Airheads Broadcasting Channel](#).

Examples

Setting two subject-alternative names for a certificate:

```
switch(config)# crypto pki certificate leaf-cert
switch (config-cert-leaf-cert)# subject-alt-name ip 2222::2222
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# subject-alt-name ip 3.3.3.3
A maximum of 2 IP addresses can be configured
```

Removing subject-alternative names from a certificate.

```
switch(config)# crypto pki certificate leaf-cert
switch (config-cert-leaf-cert)# no subject-alt-name ip 2222::2222
switch (config-cert-leaf-cert)#
switch (config-cert-leaf-cert)# no subject-alt-name ip 3.3.3.3
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Comand introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-cert-<CERT-NAME>	Administrators or local user group members with execution rights for this command.

ta-certificate

```
ta-certificate { [import [terminal]] | import {<REMOTE-URL> | <STORAGE-URL>} }
```

Description

Imports a CA certificate for use in the current TA profile. The certificate must be in PEM format. The PEM data must be delimited with these lines:

```
-----BEGIN CERTIFICATE-----  
-----END CERTIFICATE-----
```



Only the first certificate in the PEM data is imported. Any additional certificates are ignored.

Parameter	Description
<code>[import [terminal]]</code>	Import the certificate by pasting PEM-format data at the console. Upon execution, the config-cert-import context is entered for certificate pasting. To complete certificate data entry press Control-D in your terminal program. Alternatively, the pasted certificate data can include at its end the delimiter END_OF_CERTIFICATE (after the -----END CERTIFICATE----- line), making entry of Control-D unnecessary.
<code>import <REMOTE-URL></code>	Import the certificate from a file on a remote TFTP or SFTP server. The URL syntax is: <code>{tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE></code>
<code>import <STORAGE-URL></code>	Available on switch families that provide USB device file import capability, import the certificate from a file on a USB storage device inserted in the switch USB port. The URL syntax is usb:/<FILE> .

Example

Importing a certificate into the TA profile **root-cert** by pasting PEM-format certificate data at the console:

```
switch(config)# crypto pki ta-profile root-cert  
switch(config-ta-root-cert)# ta-certificate import terminal  
Paste the certificate in PEM format below, then hit enter and ctrl-D:  
switch(config-ta-cert)# -----BEGIN CERTIFICATE-----  
switch(config-ta-cert)# MIIDuTCCAqECCQCuoxeJ2ZNYcjANBgkqhkiG9w0BAQsFADCBQzELMAEBh  
switch(config-ta-cert)# VVMxEzARBgNVBAgMCKNhG1mb3JuaWExEDAOBgNVBACMB1JvY2tsDAKBg  
switch(config-ta-cert)# BAOMA0hQTjEVMBMGAlUECwwMSFBOUm9zZXZpbGx1MSowKAYDVQocG5zdz  
...  
switch(config-ta-cert)# x3WFf3dFZ8o9sd5LVAHneH/ztb9MP34z+le1V346r12L2kpxmTOVJVyTO  
switch(config-ta-cert)# BIzD/ST/HaWI+OS+S80rm93PSScEbb9GWk7vshh5EnW/moehBKcE40lzy  
switch(config-ta-cert)# 3LvMLZcssSe5J2Ca2XIhfDme8UaNZ7syGYMsAW0nG7yYHWkEOQu9s  
switch(config-ta-cert)# -----END CERTIFICATE-----  
switch(config-ta-cert)#  
The certificate you are importing has the following attributes:  
Issuer: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,  
        CN=site.com/emailAddress=test.ca@site.com  
Subject: C=US, ST=CA, L=Rocklin, O=Company, OU=Site,  
        CN=9000/emailAddress=test.ca@site.com  
Serial Number: 12121221634631568498 (0xae51217d5945772)  
  
TA certificate import is allowed only once for a TA profile  
Do you want to accept this certificate (y/n)? y  
TA certificate accepted.  
switch(config-ta-root-cert)#
```

Importing a certificate into the TA profile **root-cert2** from file **rcert2-data** on the USB device:

```
switch(config)# crypto pki ta-profile root-cert2
switch(config-ta-root-cert2)# ta-certificate import usb:/rcert2-data
The certificate you are importing has the following attributes:
Issuer: C=US, ST=California, L=Rocklin, O=Company, OU=Site,
CN=site.com/emailAddress=test.ca@site.com
Subject: C=US, ST=California, L=Rocklin, O=Company, OU=Site,
CN=9000/emailAddress=test.ca@site.com
Serial Number: 12121221634631568498 (0xae51217d5945772)

TA certificate import is allowed only once for a TA profile
Do you want to accept this certificate (y/n)? y
TA certificate accepted.
switch(config-ta-root-cert2)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-ta-<TA-NAME></code>	Administrators or local user group members with execution rights for this command.

arbitrary-label

```
arbitrary-label <LABEL>
no arbitrary-label
```

Description

Within the EST profile context, configures the generic optional label (also known as arbitrary label) to be concatenated to the EST server URL that is configured with the **url** command. There is no arbitrary label configured by default. Any existing arbitrary label is replaced by this command. The use of arbitrary labels is optional.

RFC 7030 allows the use of arbitrary labels so that one EST server may serve multiple CAs with the same server URL that gets concatenated with different arbitrary labels. The same label is used for every request made under a particular EST profile.

Some EST schemes use arbitrary labels in a more sophisticated way, defining different labels for different types of requests under the same EST profile. For example, the CA certificate request could use the generic label (configured with this **arbitrary-label** command), the certificate enrollment request could use the enrollment label (configured with the **arbitrary-label-enrollment** command), and the re-enrollment request could use the re-enrollment label (configured with the **arbitrary-label-reenrollment** command). Note that only one label of each of the three available types can be configured in any EST profile.

The **no** form of this command removes the generic arbitrary label.

Parameter	Description
<LABEL>	Specifies the generic arbitrary label. Range: Up to 64 characters.

Examples

Configuring the URL and generic arbitrary label. Note that with the URL and arbitrary label configured in this example, the final URL the switch uses to request CA certificates from the EST server is `https://est-service999.com/.well-known/est/rsa2048/cacerts`.

```
switch(config)# crypto pki est-profile EST-service1
switch(config)# url https://est-service999.com/.well-known/est
switch(config-est-EST-service1)# arbitrary-label rsa2048
```

Removing the generic arbitrary label:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# no arbitrary-label
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-est-<EST-NAME></code>	Administrators or local user group members with execution rights for this command.

arbitrary-label-enrollment

```
arbitrary-label-enrollment <LABEL>  
no arbitrary-label-enrollment
```

Description

Within the EST profile context, configures the arbitrary enrollment label to be concatenated to the EST server URL that is configured with the **url** command. This label is specific to the enrollment operation. There is no arbitrary enrollment label configured by default. Any existing arbitrary enrollment label is replaced by this command. The use of arbitrary enrollment labels is optional.

When the enrollment label is not configured, the generic arbitrary label (created with the **arbitrary-label** command) is used (if configured) for enrollment.

RFC 7030 allows the use of arbitrary labels so that one EST server may serve multiple CAs with the same server URL that gets concatenated with different arbitrary labels. The same label is used for every request made under a particular EST profile.

Some EST schemes use arbitrary labels in a more sophisticated way, defining different labels for different types of requests under the same EST profile. For example, the CA certificate request could use the generic label (configured with the **arbitrary-label** command), the certificate enrollment request could use the enrollment label (configured with this **arbitrary-label-enrollment** command), and the re-enrollment request could use the re-enrollment label (configured with the **arbitrary-label-reenrollment** command). Note that only one label of each of the three available types can be configured in any EST profile.

The **no** form of this command removes the arbitrary enrollment label.

Parameter	Description
<code><LABEL></code>	Specifies the arbitrary enrollment label. Range: Up to 64 characters.

Examples

Configuring the arbitrary enrollment label:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# arbitrary-label-enrollment ipsec-v7
```

Removing the arbitrary enrollment label :

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no arbitrary-label-enrollment
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

arbitrary-label-reenrollment

```
arbitrary-label-reenrollment <LABEL>  
no arbitrary-label-reenrollment
```

Description

Within the EST profile context, configures the arbitrary re-enrollment label to be concatenated to the EST server URL that is configured with the **url** command. This label is specific to the re-enrollment operation. There is no arbitrary re-enrollment label configured by default. Any existing arbitrary re-enrollment label is replaced by this command. The use of arbitrary re-enrollment labels is optional.

When the re-enrollment label is not configured, the generic arbitrary label (created with the **arbitrary-label** command) is used (if configured) for re-enrollment.

RFC 7030 allows the use of arbitrary labels so that one EST server may serve multiple CAs with the same server URL that gets concatenated with different arbitrary labels. The same label is used for every request made under a particular EST profile.

Some EST schemes use arbitrary labels in a more sophisticated way, defining different labels for different types of requests under the same EST profile. For example, the CA certificate request could use the generic label (configured with the **arbitrary-label** command), the certificate enrollment request could use the enrollment label (configured with the **arbitrary-label-enrollment** command), and the re-enrollment request could use the re-enrollment label (configured with this **arbitrary-label-reenrollment** command). Note that only one label of each of the three available types can be configured in any EST profile.

The **no** form of this command removes the arbitrary re-enrollment label.

Parameter	Description
<LABEL>	Specifies the arbitrary re-enrollment label. Range: Up to 64 characters.

Examples

Configuring the arbitrary re-enrollment label:

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# arbitrary-label-reenrollment ipsec-v7
```

Removing the arbitrary re-enrollment label :

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# no arbitrary-label-reenrollment
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

crypto pki est-profile

```
crypto pki est-profile <EST-NAME>
no crypto pki est-profile <EST-NAME>
```

Description

Creates a certificate Enrollment over Secure Transport (EST) profile and changes to the **config-est-<EST-NAME>** context for the profile. Each EST profile stores information about the EST service, including EST server URL Up to 16 profiles can be created.

If the specified EST profile exists, this command changes to the **config-est-<EST-NAME>** context for the profile.

The **no** form of this command deletes the specified EST profile. It also deletes the TA profiles whose CA certificates were downloaded from the corresponding EST server, and the leaf certificates that were enrolled using this EST profile.



The deletion of the related TA profiles and enrolled certificates is permanent. If the EST profile is in the startup configuration and the EST profile is deleted but this deletion is not updated in the startup configuration before a switch reboot, the EST profile will still exist after the reboot but the related TA profiles and enrolled certificates will not exist.

Parameter	Description
<code><EST-NAME></code>	Specifies the EST profile name. Range: Up to 32 alphanumeric characters (excluding ").

Examples

Creating EST profile **EST-Service1**:

```
switch(config)# crypto pki est-profile EST-Service1
switch(config-est-service1)#
```

Removing EST profile **service1**:

```
switch(config)# no crypto pki est-profile EST-Service1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

enroll est-profile

```
enroll est-profile <EST-NAME>
```

Description

Enrolls a leaf certificate through a remote EST (Enrollment over Secure Transport) server. Per RFC 7030, EST enables clients to request certificate signing services over secure TLS connections. The switch generates a key pair and the corresponding CSR. The CSR is sent to the EST server to request signing, and the signed certificate is returned to the switch where it is validated. If the whole process succeeds, the certificate can be used as a leaf certificate on the switch. When the leaf certificate approaches its expiry date, it will be renewed automatically through the same EST server.

Each enrollment or re-enrollment attempt starts with a **/cacerts** request sent to the EST server to get the latest chain of CA certificates. After the enrollment or re-enrollment succeeds, this chain of CA certificates will be compared with those downloaded previously from the same EST server. Updates will be made as appropriate.

The subject fields of the current leaf certificate must be defined before running this command. If the common name subject field is not configured, this command is rejected.

This command cannot be used to enroll or renew the default certificate "local-cert."

Note that during the enrollment initialization, if the switch detects that the EST client is associated with the device-identity certificate but the switch uses a TPM of legacy version 1.2 that is only compatible with TLS version 1.2, and TLS min-version has been set higher than 1.2, the enrollment will fail and an event like the following will be logged::

```
2025-03-10T22:55:01.525478+00:00 8320 certmgr[2465]: Event|7724|LOG_ERR|AMM|1/1|
EST client connection failed. The device-identity certificate of this system
is only compatible with TLS 1.2, but the configured TLS min-version is higher.
```

Parameter	Description
<code><EST-NAME></code>	Specifies an existing EST profile name. Range: Up to 32 alphanumeric characters (excluding ").

Example

Enrolling leaf certificate **leaf-cert1** through the EST server identified in EST profile **EST-service1**:

```
switch(config-cert-leaf-cert1)# enroll est-profile EST-service1
You are enrolling a certificate with the following attributes:
  Subject: C=US, ST=CA, L=Roseville, OU=Aruba-Roseville, O=Aruba,
          CN=leaf-cert1
  Key Type: RSA (2048 bits)

Continue (y/n)? y
Certificate enrollment via EST-service1 has been initiated.
Please use `show crypto pki certificate leaf-cert1` to check its status.

switch(config-cert-leaf-cert1)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-cert-<CERT-NAME></code>	Administrators or local user group members with execution rights for this command.

reenrollment-lead-time

reenrollment-lead-time <LEAD-TIME>
no reenrollment-lead-time

Description

Within the EST profile context, sets the certificate re-enrollment lead time which is the number of days before certificate expiry date that certificate re-enrollment will be initiated.

The **no** form of this command resets the EST server re-enrollment lead time to its default of 2 days.

Parameter	Description
<LEAD-TIME>	Specifies the certificate re-enrollment lead time in days. Range: 0 to 30 days. Default: 2 days.

Examples

Setting the certificate re-enrollment lead time to 15 days:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# reenrollment-lead-time 15
```

Resetting the certificate re-enrollment lead time to its default of 2 days :

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no reenrollment-lead-time
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

retry-count

retry-count <RETRIES>
no retry-count

Description

Within the EST profile context, sets the maximum number of retries to be attempted after the initial certificate enrollment request fails.

The **no** form of this command resets the maximum number of certificate enrollment request retries to its default of 3.

Parameter	Description
<code><RETRIES></code>	Specifies the maximum number of certificate enrollment request retries. Range: 0 to 32 retries. Default: 3 retries.

Examples

Setting the retry count to 5 retries:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# retry-count 5
```

Resetting the retry count to its default of 3 retries:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no retry-count
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config-est-<EST-NAME></code>	Administrators or local user group members with execution rights for this command.

retry-interval

```
retry-interval <INTERVAL>  
no retry-interval
```

Description

Within the EST profile context, sets the interval at which a failed certificate enrollment request is retried. The **no** form of this command resets the enrollment request retry interval to its default of 30 seconds.

Parameter	Description
<code><INTERVAL></code>	Specifies the enrollment request retry interval in seconds. Range: 30 to 600 seconds. Default: 30 seconds.

Examples

Setting the certificate enrollment request retry interval to 45 seconds:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# retry-interval 45
```

Resetting the retry interval to its default of 30 seconds:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no retry-interval
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est- <i><EST-NAME></i>	Administrators or local user group members with execution rights for this command.

show crypto pki est-profile

```
show crypto pki est-profile [<EST-NAME>]
```

Description

Shows a list of all configured EST profiles, or detailed information for a specific profile.

Parameter	Description
<i><EST-NAME></i>	Specifies the EST profile name. Range: Up to 32 alphanumeric characters (excluding ").

Examples

Showing a list of all configured EST profiles:

```
switch# show crypto pki est-profile  
  
Profile Name          Downloaded  Enrolled  
TA Profiles  Certificates  
-----  
EST-service1         2           3  
EST-service2         1           2  
EST-service3         2           0
```

Showing detailed information for EST profile **EST-service1**:

```
switch# show crypto pki est-profile EST-service1
Profile Name           : EST-service1
Service VRF           : mgmt
Service URL            : https://est-service999.com
Arbitrary Label        : not configured
Arbitrary Label Enrollment : /ipsec-VP7
Arbitrary Label Reenrollment : not configured
Authentication Username : est1
Authentication Password :
  AQBapREALpWYm2z7L1LanOtR3vGkqhBN1hBUU2CuvQXUF/ggYgAAnAnGTnKq49P4c
  dNQ6UqPbjHL4XzCO0T04djkhsUXPKGfnsWuFEONveh+JbEobqKImfwJjc3eWHiaUb
  eNpPx2zN2Q1DdyxAAQi4rmKr8LITMTTMD7qr
Retry Interval         : 45 seconds
Retry Count            : 5 times
Reenrollment Lead Time : 2 days
Downloaded TA Profiles : 2
Enrolled Certificates  :
  leaf-cert1
  leaf-cert2
  leaf-cert3
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

url

```
url <URL>
no url
```

Description

Within the EST profile context, configures the URL of the certificate enrollment EST server. This is not configured by default. Any existing URL is replaced by this command.

The **no** form of this command removes the EST server URL within the selected EST profile. The removal of the URL does not affect the TA profiles and enrolled certificates from the EST server.

Parameter	Description
<URL>	Specifies the EST server URL. Range: Up to 192 characters.

Usage

- The configuration and update of the EST profile URL triggers the sending of a **/cacerts** request to the EST server. A successful request will result in a chain of trusted CA certificates being downloaded from the EST server. Each CA certificate, either root CA certificates or intermediate CA certificates, will be saved as a TA profile, with TA profile name **<est-name>-est-taNN** with **NN** representing two numerical digits. This TA profile naming scheme with the **-est-taNN** suffix is reserved for TA profiles downloaded from EST servers.
- Upon connection with an EST server, the switch authenticates the server by validating the server certificate. For this validation to succeed, a TA profile needs to pre-exist in the switch with a CA certificate from the issuer chain of the server certificate. Once the server is authenticated, all CA certificates in its **/cacerts** response will be trusted, with no further validation occurring for them.
- The TA profiles with CA certificates downloaded from an EST server will have their revocation check set to OCSP, enforcement set to optional, and the OCSP VRF set to the same as that of the EST profile.

Examples

Configuring the EST server URL:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# url https://est-service999.com/.well-known/est
```

Removing the EST server URL:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no url
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

username

```
username <USERNAME> password [ciphertext <CIPHERTEXT-PASSWORD> |  
plaintext <PLAINTEXT-PASSWORD>]  
no username
```

Description

Within the EST profile context, configures the user account information for the EST server that is used to authenticate the switch before accepting requests from the switch. This is not configured by default. Any existing username and password is replaced by this command.

When entered without either optional **ciphertext** or **plaintext** parameters, the plaintext password is prompted for twice, with the characters entered masked with "*" symbols.

The **no** form of this command removes the user account information within the selected EST profile.

There are two ways the EST client on a CX switch can prove itself to an EST server: a certificate, and/or username and password. At least one of the two must be configured for the EST request to succeed. If both are configured, certificate authentication will be used. If a certificate is not configured or certificate authentication fails, and username and password is configured, the username and password will be sent to the EST server for authentication.

Parameter	Description
<code><USERNAME></code>	Specifies the EST server account user name. The exact user name requirements are set by the chosen EST service. Range: Up to 32 alphanumeric characters.
<code>ciphertext <CIPHERTEXT-PASSWORD></code>	Specifies the EST server account password as Base64 ciphertext. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. NOTE: The ciphertext password must be gotten from the EST service.
<code>plaintext <PLAINTEXT-PASSWORD></code>	Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. The exact password requirements are set by the chosen EST service. Range: Up to 64 alphanumeric characters.

Examples

Configuring an EST user with prompted cleartext password entry :

```
switch(config)# crypto pki est-profile EST-service1
switch(config-est-EST-service1)# username est1 password
Enter password: *****
Confirm password: *****
switch(config-est-EST-service1)#
```

Configuring an EST user with direct cleartext password entry:

```
switch(config)# crypto pki est-profile EST-service2
switch(config-est-EST-service2)# username est1 password plaintext concept_leap739
```

Configuring an EST user with ciphertext password entry :

```
switch(config)# crypto pki est-profile EST-service3
switch(config-est-EST-service3)# username est1 password ciphertext
AQBpRALpWYm2z7L1LanOtR3vGkqhN1hBU2CuvQXUF/ggYgAAAHWaPqxU6nAnGTnKq49P4cdNQ6U
```

```
qPbjHL4XzO0T04djkUPKGfnsWuFEONveh+JbEobq63+1k80qBKImfwJjc3eWHiaUbeNpPx2zN2Q  
1DdyxAAQi4rmKr8LITMTMd7qr
```

Removing the EST user account information for EST profile EST-service2:

```
switch(config)# crypto pki est-profile EST-service2  
switch(config-est-EST-service2)# no username
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

vrf

```
vrf <VRF-NAME>  
no vrf
```

Description

Within the EST profile context, selects the VRF through which the EST server can be reached. Any existing VRF selection is replaced by this command. When this command is not used, VRF **mgmt** is used by default on switch families supporting the **mgmt** VRF, otherwise the default VRF named **default** is used.

The **no** form of this command selects the default VRF either **mgmt** or **default**.

Parameter	Description
<VRF-NAME>	Specifies the name of the VRF to use for EST server communication.

Examples

Selecting VRF **it-services** for EST server communications:

```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# vrf it-services
```

Resetting the VRF to its default of **mgmt** for EST server communications:


```
switch(config)# crypto pki est-profile EST-service1  
switch(config-est-EST-service1)# no vrf
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-est-<EST-NAME>	Administrators or local user group members with execution rights for this command.

Chapter 99

Port filtering commands

clear ptp statistics

clear ptp statistics [<IFNAME>]

Description

Clears PTP counters for the given interface.

Parameter	Description
<IFNAME>	Optional: Specifies the interface name.

Examples

Clearing PTP counters for the given interface:

```
switch# clear ptp statistics 1/1/8
switch# clear ptp statistics lag1
switch# clear ptp statistics
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Administrators or local user group members with execution rights for this command.

clock-domain

clock-domain <DOMAIN-NUMBER>
no clock-domain <DOMAIN-NUMBER>

Description

Configures the PTP clock domain to a specified value.

The **no** form of this command removes the PTP domain configuration of the PTP clock.

Parameter	Description
<code><DOMAIN-NUMBER></code>	Sets the PTP clock domain. Range: 0 to 254. Value configurable subject to limits established by the PTP profile.

Usage

- The one-step end-to-end transparent clock works across domains.
- For boundary clocks, the clock-domain has to be identical with the domain used in the network.
- All PTP devices must be within same domain to be able to sync with each other.
- This command is only enabled in the PTP profile context.
- For PTP transparent clock, you must configure the same clock-domain as on clients and GM to synchronize.

Examples

Entering the PTP profile context and setting the PTP clock domain value:

```
switch(config)# ptp profile 1588v2  
switch(config-ptp)#clock-domain 4
```

Removing the PTP clock domain value:

```
switch(config-ptp)# no clock-domain
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

clock-step

```
clock-step {one-step|two-step}  
no clock-step {one-step|two-step}
```

Description

Configures the clock step mode that determines when the egress-time information is sent. The 8325P and 9300 Switch Series only support the one-step command. The **no** form of this command removes the PTP clock-step configuration of the PTP clock.

Parameter	Description
one-step	Sets the PTP clock-step mode to one-step messaging in which egress-time information is sent along with the SYNC message.
two-step	Sets the PTP clock-step mode to two-step messaging in which egress-time information is sent a subsequent follow-up message with the egress timestamp of the previously sent SYNC message.

Usage

- Mandatory command to start the PTP clock.
- Boundary clocks can inter-operate with different step modes upstream or downstream.

Example

Setting the clock-step mode to one-step messaging:

```
switch(config-ptp) # clock-step one-step
```

Removing the clock-step mode configuration:

```
switch(config-ptp) # no clock-step
```

Setting the clock-step mode to two-step messaging:

```
switch(config-ptp) # clock-step two-step
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

enable

enable
no enable

Description

Enables the PTP profile globally. However, the PTP clock is started only when all the mandatory commands are set.

The **no** form of this command disables the PTP profile globally.

Usage

Mandatory command to start the PTP clock.

Examples

Enabling the PTP profile:

```
switch(config)# ptp profile 1588v2  
switch(config-ptp)# enable
```

Disabling the PTP profile:

```
switch(config)# ptp profile 1588v2  
switch(config-ptp)# no enable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

ip source-interface

```
ip source-interface {ptp | all} interface <IFNAME> [vrf <VRF-NAME>  
ip source-interface {ptp | all} <IPV4-ADDR> [vrf <VRF-NAME>]  
no ip source-interface {ptp | all} interface <IFNAME> [vrf <VRF-NAME>  
no ip source-interface {ptp | all} <IPV4-ADDR> [vrf <VRF-NAME>]
```

Description

Configures the source IP address to be used when sending PTP messages. Use the `ptp` keyword to set source IP address specific to the PTP feature. If the feature-specific configuration is not available, the source IP address corresponding to the `all` option will be used.

The `no` form of this command removes the configuration of the source IP address used by the PTP feature.

Parameter	Description
<code>ptp</code>	Selects the PTP protocol.
<code>all</code>	Selects all protocols that can be configured by this command.
<code>interface <IF-NAME></code>	Specifies the name of the interface from which the source IP address is obtained. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.
<code>vrf <VRF-NAME></code>	Specifies the VRF name.
<code><IPv4-ADDR></code>	Specifies the source IPv4 address to be used. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the default VRF, if the <code>vrf</code> option is not used). Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Usage

- This command must be configured on the switch when PTP is enabled on VLAN trunk or access ports, and the transport protocol is IPv4.
- In the current version of PTP, only the default VRF is supported.
- This command is not applicable to the end-to-end transparent clock.

Examples

Configuring the source IP address for sending PTP messages:

```
switch(config)# ip source-interface ptp interface 1/1/1
switch(config)# ip source-interface ptp 10.10.10.1
switch(config)# ip source-interface ptp interface vlan10
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config	Administrators or local user group members with execution rights for this command.

mode

```

mode boundary {end-to-end | peer-to-peer}
no mode boundary {end-to-end | peer-to-peer}
mode transparent {end-to-end | peer-to-peer}
no mode transparent {end-to-end | peer-to-peer}

```

Description

Configures the switch PTP clock mode, either boundary or transparent, with a delay-request mechanism of either end-to-end or peer-to-peer. A device in transparent clock mode does not synchronize (syntonize) itself to a grandsource clock. The 9300 and 8325P Switch Series support the **mode boundary end-to-end** command only.

The **no** form of this command unconfigures the PTP clock mode and delay-request mechanism.

Parameter	Description
boundary	Selects boundary clock mode.
transparent	Selects transparent clock mode.
end-to-end	Selects the end-to-end delay-request mechanism.
peer-to-peer	Selects the peer-to-peer delay-request mechanism. Not supported with VSF.

Examples

Configuring PTP boundary clock mode with the end-to-end delay-request mechanism:

```
switch(config-ptp)# mode boundary end-to-end
```

Unconfiguring PTP boundary clock mode with the end-to-end delay-request mechanism:

```
switch(config-ptp)# no mode boundary end-to-end
```

Configuring PTP boundary clock mode with the peer-to-peer delay-request mechanism:

```
switch(config-ptp)# mode boundary peer-to-peer
```

Unconfiguring PTP boundary clock mode with the peer-to-peer delay-request mechanism:

```
switch(config-ptp)# no mode boundary peer-to-peer
```

Configuring PTP transparent with the end-to-end delay-request mechanism:


```
switch(config-ptp) # mode transparent end-to-end
```

Unconfiguring PTP transparent with the end-to-end delay-request mechanism:

```
switch(config-ptp) # no mode transparent end-to-end
```

Configuring PTP transparent with the peer-to-peer delay-request mechanism:

```
switch(config-ptp) # mode transparent peer-to-peer
```

Unconfiguring PTP transparent with the peer-to-peer delay-request mechanism:

```
switch(config-ptp) # no mode transparent peer-to-peer
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Added support for mode boundary end-to-end on the 9300.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

priority1

```
priority1 <PRIORITY>  
no priority1 <PRIORITY>
```

Description

Configures the PTP clock **priority1** value of the device. This value is operational when the device is in boundary clock mode and participating in the Best Clock Source Algorithm (BMCA). This value is used to indicate priority to its downstream clock-aware devices.

The **no** form of this command removes the PTP **priority1** configuration of the PTP clock and sets it to the default value of 128.

Parameter	Description
<PRIORITY>	Sets the priority value. Default 128.

Usage

This value can be configured only for the boundary clock.

Examples

Configuring PTP priority1 value:

```
switch(config-ptp) # priority1 129
```

Removing PTP priority1 configuration:

```
switch(config-ptp) # no priority1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

priority2

```
priority2 <PRIORITY>  
no priority2 <PRIORITY>
```

Description

Configures the PTP clock **priority2** value of the device. This value is operational when the device is in boundary clock mode and participating in the Best Clock Source Algorithm (BMCA). This value is used to indicate priority to its downstream clock-aware devices.

The **no** form of this command removes the PTP **priority2** configuration of the PTP clock and sets it to the default value of 128.

Parameter	Description
<PRIORITY>	Sets the priority value. Default 128.

Usage

This value can be configured only for the boundary clock.

Examples

Configuring PTP `priority2` value:

```
switch(config-ptp)# priority2 129
```

Removing PTP `priority2` configuration:

```
switch(config-ptp)# no priority2
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

ptp announce-interval

```
ptp announce-interval {1588v2 | aes67 | aes-r16 | dot1as | smpte} <LOG-SECONDS>  
no ptp announce-interval {1588v2 | aes67 | aes-r16 | dot1as | smpte}
```

Description

Sets the announce message transmit interval on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command removes the announce message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

Parameter	Description
1588v2	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default: 1.
aes67	Specifies the PTP AES67 profile timers. Range: 0 to 1. Default: 1.
aes-r16	Specifies the PTP AES-R16 profile timers. Range: 0 to 1. Default: 1.
dot1as	Specifies the PTP 802.1AS profile timers. Range: -6 to 1. Default: 0.
smpte	Specifies the PTP SMTPE profile timers. Range: -3 to 1. Default: 0.
<LOG-SECONDS>	Sets the announce message interval in log seconds.

Switch series	Supported profiles
9300-32D	1588v2, smpte

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP 1588v2 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-interval 1588v2 1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp announce-timeout

```
ptp announce-timeout {1588v2|aes67|aes-r16|dot1as|smpte} <COUNT>
no ptp announce-timeout {1588v2|aes67|aes-r16|dot1as|smpte}
```

Description

Sets the announce message receipt timeout on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command resets the announce message receipt timeout configuration on a PTP-enabled interface and sets a profile-specific default value.

Parameter	Description
1588v2	Specifies the PTP 1588v2 profile timers. Range: 2-255. Default: 3.
aes67	Specifies the PTP AES67 profile timers. Range: 2-10. Default: 3.
aes-r16	Specifies the PTP AES-R16 profile timers. Range: 2-10. Default: 3.

Parameter	Description
dot1as	Specifies the PTP 802.1AS profile timers. Range: 2-255. Default: 3.
smp te	Specifies the PTP SMPTE profile timers. Range: 2-10. Default: 3.
<COUNT>	Specifies the number of announcement intervals.

Switch series	Supported profiles
9300-32D	1588v2, smp te

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP 1588v profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-timeout 1588v2
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp clock-source-only

```
ptp clock-source-only
no ptp clock-source-only
```

Description

Configures the PTP port state to clock_source state. This prohibits the port from entering into a clock_sink or passive state.

The **no** form of this command removes the clock_source state configuration on the port and returns it to normal BMCA operation.

Usage

This can only be configured for the boundary clock.

Examples

Configuring the clock_source only role for the port:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp clock-source-only
```

Removing the configuration of clock_source only role for the port:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp clock-source-only
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp delay-req-interval

```
ptp delay-req-interval {1588v2 | aes67 | aes-r16 | smpte} <LOG-SECONDS>
no ptp delay-req-interval {1588v2 | aes67 | aes-r16 | smpte}
```

Description

Sets the delay_req message transmit interval on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command removes the delay_req message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

Parameter	Description
1588v2	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default 0.
aes67	Specifies the PTP AES67 profile timers. Range: -3 to 1. Default 0.
aes-r16	Specifies the PTP AES-R16 profile timers. Range: 0 to 1. Default 0.
smpte	Specifies the PTP SMTPE profile timers. -7 to 1. Default -3.

Parameter	Description
<LOG-SECONDS>	Sets the delay_req message interval in log seconds.

Switch series	Supported profiles
9300-32D	1588v2, smpte

Usage

- Use this command for end-to-end (E2E) mode and use command **ptp pdelay-interval** for peer-to-peer mode.
- This command is only for boundary clock.

Examples

Setting the PTP 1588v2 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp delay-req-interval 1588v2 2
```

Removing a PTP 1588v2 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp delay-req-interval 1588v2
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp enable

```
ptp enable
no ptp enable
```

Description

Enables PTP on the interface. The **no** form of this command disables PTP on the interface. PTP can be enabled only on physical L2 or L3 interfaces and LAG L2 or L3 interfaces.

Examples

Enabling PTP on a physical interface:

```
switch(config)# interface 1/1/1  
switch(config-if)# ptp enable
```

Disabling PTP on the interface context:

```
switch(config)# interface 1/1/1  
switch(config-if)# no ptp enable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp lag-role

```
ptp lag-role {primary | secondary}  
no ptp lag-role {primary | secondary}
```

Description

Configures the PTP role for the member interfaces of a Link Aggregation (LAG) . When there are two or more member interfaces for a LAG, only one link can be configured as primary and only one other link can be configured as secondary. The primary member interface is used for transmitting the PTP packets generated by the boundary clock. When the primary member goes down, the secondary member is used for PTP packet transmission. If both primary and secondary members go down, PTP does not flip over to the other links of the LAG.

The **no** form of this command removes the PTP role configuration for the LAG member interface.



This command is not supported when configured as a transparent clock.

Parameter	Description
primary	Sets the primary PTP lag-role for the LAG member interface.
secondary	Sets the secondary PTP lag-role for the LAG member interface.

Usage

- LAG roles must be configured for boundary clock.
- For the primary or secondary LAG roles, ensure that the same link ports are configured on both ends of the LAG.

Examples

Setting the primary PTP lag-role for the LAG member interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp lag-role primary
```

Setting the secondary PTP lag-role for the LAG member interface:

```
switch(config)# interface 1/1/2
switch(config-if)# ptp lag-role secondary
```

Removing the PTP lag-role configuration for the LAG member interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp lag-role
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp peer ip

```
ptp peer ip <IP-ADDRESS>
no ptp peer ip <IP-ADDRESS>
```

Description

Configures destination IP addresses for the interfaces in unicast transmission.

The **no** form of this command removes the PTP destination IP address configuration for the interfaces in unicast transmission.



Unicast and multicast configurations are mutually exclusive. If a unicast port is configured, all multicast ports will cease operating. If multicast transmission is desired no unicast ports can be configured.

Parameter	Description
<code>ip <IP-ADDRESS></code>	Specifies the peer IPv4 address. Syntax: A.B.C.D

Usage

- This command has no effect when configured as a transparent clock.

Example

Configuring `ptp peer ip` on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp peer ip 10.0.0.1
```

Removing `ptp peer ip` on the interface:

```
switch(config-if)# no ptp peer ip 10.0.0.1
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	<code>config-if</code>	Administrators or local user group members with execution rights for this command.

ptp profile

```
ptp profile {<PROFILE NAME>}
no ptp profile {<PROFILE NAME>}
```

Description

Enters the PTP context to configure the PTP profile in which the device will operate. Configure a PTP profile before configuring mode or other profile-specific parameters. The device can be operating in any one profile at a given point of time.

The **no** form of this command removes the PTP profile configuration in which the device will operate. This command clears the PTP profile and all parameters related to that profile.

Parameter	Description
<code><PROFILE NAME></code>	Specifies the profile to be used. Profiles include: ▪ 1588v2: Specifies the IEEE 1588-2008 profile to be used. ▪ smpte: Specifies the IEEE SMPTE-ST-2059-2 profile to be used.
Switch series	Supported profiles
9300-32D	1588v2, smpte

Usage

Configure PTP profile before configuring mode or other profile-specific parameters.

Example

Configuring PTP profile **1588v2**:

```
switch(config)# ptp profile 1588v2
```

Configuring PTP profile **smpte**:

```
switch(config)# ptp profile smpte
```

Configuring more than one PTP profile:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# exit
switch(config)# ptp profile smpte
switch(config-ptp)#
The existing profile must be removed using the 'no ptp profile' command before
configuring a different profile.
```

Removing the PTP profile:

```
switch(config-ptp)# no ptp profile
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Support added for the 1588v2 and SMPTE profiles on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config	Administrators or local user group members with execution rights for this command.

ptp sync-interval

```
ptp sync-interval {1588v2 | dot1as | aes67 | smpte} <LOG-SECONDS>  
no ptp sync-interval {1588v2 | dot1as | aes67 | smpte}
```

Description

Sets the sync message transmit interval on a PTP-enabled interface for a specific PTP profile. The **no** form of this command removes the sync message transmit interval configuration on a PTP enabled interface and sets it to a profile-specific default value.

Parameter	Description
1588v2	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default 0.
dot1as	Specifies the PTP 802.1 AS profile timers. Range: -6 to 1. Default -3.
aes67	Specifies the PTP AES67 profile timers. Range: -4 to 1. Default -3.
smpte	Specifies the PTP SMPTE profile timers. Range: -7 to -1. Default -3.
<LOG-SECONDS>	Sets the sync message interval in log seconds.

Switch series	Supported profiles
9300-32D	1588v2, smpte

Examples

Setting the PTP SMPTE sync interval :

```
switch(config)# interface 1/1/1  
switch(config-if)# ptp sync-interval smpte -2
```

Setting the PTP 1588v2 sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval 1588v2 -3
```

Setting the PTP AES67 sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval aes67 -2
```

Removing the PTP AES67 sync interval:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp sync-interval aes67
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

ptp vlan

```
ptp vlan <VLAN-ID>
no ptp vlan <VLAN-ID>
```

Description

Configures a VLAN for PTP messages. It is necessary when the boundary clock port is a VLAN trunk L2 interface (**no routing**).

The **no** form of this command removes the VLAN configuration for PTP messages.

Parameter	Description
<VLAN-ID>	

Usage

- This configuration has no bearing on only one-step transparent clock end-to-end. **Ptp peer-to-peer vlan** will be configured on transparent clock peer-to-peer mode.

- In boundary clock mode, only PTP packets in PTP VLAN are processed; PTP packets from other VLANs are dropped.
- **ptp vlan** should be configured on interfaces only when the specific VLAN is a trunk/tagged member of that port. This configuration should not be performed on an access port.

Examples

Configuring VLANs 4 and 5 for PTP messages:

```
switch(config)# interface 1/1/1  
switch(config-if)# ptp vlan 4,5
```

Configuring VLANs 2 through 5 for PTP messages:

```
switch(config)# interface 1/1/1  
switch(config-if)# ptp vlan 2-5
```

Removing the VLAN configuration for PTP messages:

```
switch(config)# interface 1/1/1  
switch(config-if)# no ptp vlan
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.17	Multi-VLAN support added.
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.

show ptp clock

```
show ptp clock
```

Description

Shows PTP clock-related information.

Example

Showing PTP clock information:

```
switch# show ptp clock
PTP Profile           : 1588v2
PTP Mode             : boundary
Delay Mechanism       : end-to-end
Clock Identity        : 08:00:11:FF:FE:21:E4:46
Network Transport Protocol : ethernet
Clock Step           : Two
Clock Domain         : 0
Number of PTP Ports  : 2
Priority1             : 246
Priority2             : 248

Clock Quality :
  Class        : 248
  Accuracy     : 32
  Offset (log variance) : 16640

Offset From Clock-Source : +0.000000000 (s)
Mean Delay               : +0.000000000 (s)
Steps Removed           : 0
PTP Clock                : Thu Dec 10 13:21:01.413 2020
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp foreign-clock-sources

show ptp foreign-clock-sources

Description

Shows the priority1, priority2, class, accuracy, offset-scaled-log-variance (OSLV), and steps removed information for foreign clock-source nodes.

Example

Showing PTP foreign clock-source information:

```
switch# show ptp foreign-clock-sources
P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-scaled-log-variance, SR=Steps-removed, V=VLAN Identifier
```

Interface	Foreign Port ID	Clock Source ID	P1	P2	C	A	OSLV	SR
1/1/1	00:fd:45:ff:fe:67:d5:c0(0x0001)	00:50:56:ff:fe:bd:7b:ff	128	128	13	254	65535	2



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp interface

```
show ptp interface [<IFNAME> | profile-data | dotlas | brief]
```

Description

Shows PTP port-related information.



When PTP is enabled on a VSF stack it is automatically enabled by default on all VSF interfaces.

Parameter	Description
<IFNAME>	Specifies the interface name.
profile-data	Shows additional information of the profile.
dotlas	Shows port data specific to the 802.1 AS profile.
brief	Shows information in a brief format.

Examples

Showing PTP port information when the switch is acting as a transparent clock:


```

switch# show ptp interface 1/1/1
Port Identity           : 00:00:00:00:00:00:00:00 (0x0000)
Port Number             : 0
PTP Version             : 2
PTP Enable              : Enabled
PTP Transport           : ipv4
Port State              : Disabled
Delay Mechanism          : peer-to-peer
Announce Interval (log mean) : 0
Announce Receipt Timeout : 0
Sync Interval (log mean)  : 0
Sync Timeout            : NA
Delay Request Interval (log mean) : NA
Peer Delay Request Interval (log mean) : 0
Mean Path Delay         : 0 (ns)
switch#

```

```

switch# show ptp interface lag20
Port Identity           : NA
Port Number             : NA
PTP Version             : 2
PTP Enable              : Enabled
Transport of PTP        : ipv4
Port State              : NA
Delay Mechanism          : end-to-end
Announce Interval (log mean) : NA
Announce Receipt Timeout : NA
Sync Interval (log mean)  : NA
Sync Timeout            : NA
Delay Request Interval (log mean) : N
Peer Delay Request Interval (log mean) : 0
Mean Path Delay         : 0 (ns)

```

Showing PTP port information when the switch is acting as a boundary clock:

```

switch# show ptp interface 1/1/1
Interface : 1/1/1
Port Identity           : 88:3a:30:ff:fe:05:c9:80 (port: 0x0002)
Port Number             : 2
PTP Version             : 2
PTP Enable              : Enabled
Transport of PTP        : ethernet
Port State              : Clock Source
Delay Mechanism          : end-to-end
Announce Interval (log mean) : 0
Announce Receipt Timeout : 3
Sync Interval (log mean)  : -3
Sync Timeout            : NA
Delay Request Interval (log mean) : 0
Peer Delay Request Interval (log mean) : 0
Mean Path Delay         : 0 (ns)

```

```

switch# show ptp interface lag1
Port Identity           : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number             : 2
PTP Version             : 2
PTP Enable              : Enabled
Transport of PTP        : ipv4
Port State              : Clock Source
Delay Mechanism          : end-to-end
Announce Interval (log mean) : 0

```

```

Announce Receipt Timeout      : 3
Sync Interval (log mean)     : -3
Sync Timeout                  : NA
Delay Request Interval (log mean) : -3
Peer Delay Request Interval (log mean) : 0
Mean Path Delay               : 0 (ns)
Primary Interface             : 1/1/5
Secondary Interface           : 1/1/6

switch# show ptp interface
Interface lag20:
Port Identity                  : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                    : 2
PTP Version                    : 2
PTP Enable                     : Enabled
Transport of PTP               : ipv4
Port State                     : Clock Source
Delay Mechanism                 : end-to-end
Announce Interval (log mean)   : 0
Announce Receipt Timeout       : 3
Sync Interval (log mean)       : -3
Sync Timeout                   : NA
Delay Request Interval (log mean) : -3
Peer Delay Request Interval (log mean) : 0
Mean Path Delay                : 0 (ns)
Primary Interface              : 1/1/5
Secondary Interface            : 1/1/6

Member Interface 1/1/5:
Port Identity                  : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                    : 2
PTP Version                    : 2
PTP Enable                     : Enabled
Transport of PTP               : ipv4
Port State                     : Running
Delay Mechanism                 : end-to-end
Announce Interval (log mean)   : 0
Announce Receipt Timeout       : 3
Sync Interval (log mean)       : -3
Sync Timeout                   : NA
Delay Request Interval (log mean) : -3
Peer Delay Request Interval (log mean) : 0
Mean Path Delay                : 0 (ns)

Member Interface 1/1/6:
Port Identity                  : 00:fd:45:ff:fe:68:f3:00 (port: 0x0003)
Port Number                    : 3
PTP Version                    : 2
PTP Enable                     : Enabled
Transport of PTP               : ipv4
Port State                     : Not Running
Delay Mechanism                 : end-to-end
Announce Interval (log mean)   : 0
Announce Receipt Timeout       : 3
Sync Interval (log mean)       : -3
Sync Timeout                   : NA
Delay Request Interval (log mean) : -3
Peer Delay Request Interval (log mean) : 0
Mean Path Delay                : 0 (ns)

Interface 1/1/15:
Port Identity                  : 00:fd:45:ff:fe:68:f3:00 (port: 0x0001)

```

```

Port Number                : 1
PTP Version                : 2
PTP Enable                 : Enabled
Transport of PTP           : ipv4
Port State                 : Clock Sink
Delay Mechanism             : end-to-end
Announce Interval (log mean) : 0
Announce Receipt Timeout   : 3
Sync Interval (log mean)   : -3
Sync Timeout               : NA
Delay Request Interval (log mean) : -3
Peer Delay Request Interval (log mean) : 0
Mean Path Delay            : 0 (ns)

```

Showing PTP port information in a brief format when the switch is acting as a boundary clock:

```

switch# show ptp interface brief
Interface      PTP State
-----
1/1/11         Clock Sink
1/1/12         Clock Source
1/1/15         Clock Source
1/1/16         Clock Source

```

Showing PTP port information of 802.1AS profile:

```

switch# show ptp int 1/1/1 profile-data dot1as
asCapable      : TRUE
Compute Neighbor RateRatio : TRUE
Neighbor RateRatio : 1.2
Compute Neighbor PropDelay : TRUE
Neighbor Propagation Delay : 35 ns
PDelay Lost Response Threshold : 3
Lost Response Threshold Exceeded : FALSE

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp parent

```
show ptp parent
```

Description

Shows parent node information for the PTP device.

Example

Showing PTP parent node information:

```
switch# show ptp parent
PTP Parent Properties

Parent Clock
-----
Parent Clock Identity           : 00:00:00:00:00:00:01
Parent Port Number              : 0x0001
Observed Parent Offset (log variance) : 65535
Observed Parent Clock Phase Change Rate: 2147483647

Grandsource Clock
-----
Grandsource Clock Identity      : 00:00:00:00:00:00:01
Grandsource Clock Quality
  Class                         : 6
  Accuracy                      : 35
  Offset (log variance)         : 0
Priority1                       : 0
Priority2                       : 0
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp time-property

```
show ptp time-property
```

Description

Shows PTP clock-time properties for the PTP device.

Parameter	Description

Example

Showing PTP clock time properties:

```
switch # show ptp time-property
PTP Clock Time Property
-----
Current UTC Offset Valid : FALSE
Current UTC Offset      : 37
Leap59                  : FALSE
Leap61                  : FALSE
Time Traceable          : FALSE
Frequency Traceable     : FALSE
PTP Timescale           : FALSE
Synchronization Uncertain : FALSE
Time Source             : 160
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show running-config ptp

```
show running-config ptp
```

Description

Shows PTP running configuration related information.

Example

Showing PTP running configuration information:

```
switch# show running-config ptp
ptp profile smpte
  enable
  clock-step two-step
  transport-protocol ipv4
  mode boundary peer-to-peer
interface 1/1/15
  no shutdown
```

```
ip address 30.1.1.1/16
ptp enable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.

Command Information

Platforms	Command context	Authority
9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

transport-protocol

```
transport-protocol {ethernet | ip | udp <UDP-PORT>}
no transport-protocol
```

Description

Sets the transport protocol for PTP packets. In the case of IPv4, the UDP check-sum is reset. There is no default transport-protocol.

The **no** form of this command disconnects the clock from its source.

Parameter	Description
ethernet	Specifies the Ethernet (Layer 2) transport protocol.
ip	Specifies the IPv4 transport protocol.
udp	Specifies the UDP transport protocol.
<UDP-PORT>	Specifies the transport layer port. Range: 1-65355. The default is 4739.

Usage

Mandatory command to start the PTP clock.

Example

Setting the Ethernet transport protocol for PTP packets:

```
switch(config-ptp) # transport-protocol ethernet
```

Removing the transport protocol for PTP packets:

```
switch(config-ptp) # no transport-protocol
```

Setting the transport protocol for exporter-1 to UDP with port 2055:

```
switch(config) # flow exporter exporter-1  
switch(config-flow-exporter) # transport udp 2055
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.14.1000	Command introduced on the 9300 Switch Series.
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.

Command Information

Platforms	Command context	Authority
9300	config-ptp	Administrators or local user group members with execution rights for this command.

apply qos

```
apply qos [queue-profile <QUEUE-NAME>] schedule-profile <SCHEDULE-NAME>
no apply qos [queue-profile <QUEUE-NAME>] schedule-profile <SCHEDULE-NAME>
```

Description

Applies a queue profile and schedule profile globally to all Ethernet and LAG interfaces on the switch, or applies a schedule profile to a specific interface. When applied globally, the specified schedule profile is configured only on Ethernet interfaces and LAGs that do not already have their own schedule profile. The same profile can be applied both globally and locally to an interface. This guarantees that an interface always uses the specified profile, even if the global profile is changed.

The **no** form of this command removes the specified schedule profile from an interface and the interface uses the global schedule profile. This is the only way to remove a schedule profile override from the interface.



When applying QoS settings to a port configured to support priority-based flow control, specific configuration settings must be respected when defining a CoS map and queue profile. See the command **flow-control** in the *Command-Line Interface Guide* for details.



Interfaces may shut down briefly during reconfiguration.

Parameter	Description
queue-profile <QUEUE-NAME>	Specifies the name of the queue profile to apply. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-). This parameter is not supported in the config-if context.
schedule-profile <SCHEDULE-NAME>	Specifies the name of the schedule profile to apply. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Usage

- The switch must always have a globally-applied queue and schedule profile. To stop using a given profile, apply a different profile.
- For a queue profile to be complete and ready to be applied, all eight local priorities must be mapped to a queue.

- For a schedule profile to be complete and ready to be applied, it must define all queues specified in the queue profile. All queues must use the same algorithm, except for the highest numbered queue, which can be **strict**.
- Both the queue profile and the schedule profile must specify the same number of queues.
- Schedule profiles can be modified while applied, but only in ways where a single command will not result in the profile becoming invalid. For example, queue 7 can have the algorithm changed, and weighted queues can have their weights changed.

If there are interfaces running with priority-based flow control (PFC) and a new queue profile to be applied maps a local-priority used by the PFC traffic to another queue, the following steps are required:

1. Shutdown all interfaces
2. Apply the new queue profile
3. Save the configuration to startup
4. Reboot the switch

If the new queue profile was applied before shutting down the PFC interfaces then PFC traffic will still use the same queue from the previous profile until the switch is rebooted.

If the number of queues was changed from the previous queue profile to the new one, any Ethernet or LAG interfaces with locally applied schedule profiles will program the newly applied global schedule-profile. The *show running-config interface* command will list the existing *apply qos schedule-profile* command with a comment describing the actual profile applied:

```
apply qos schedule-profile Old_Schedule
!actual schedule-profile New_Schedule
```

Examples

The following commands illustrate a valid configuration where every local priority value is assigned to a queue and all assigned queues are defined:

```
switch(config)# qos cos-map 1 local-priority 1
switch(config)# qos queue-profile Q1
switch(config)# map queue 0 local-priority 0
switch(config)# map queue 1 local-priority 1
switch(config)# map queue 2 local-priority 2
switch(config)# map queue 3 local-priority 3
switch(config)# map queue 4 local-priority 4
switch(config)# map queue 5 local-priority 5
switch(config)# map queue 6 local-priority 6
switch(config)# map queue 7 local-priority 7
switch(config)# qos schedule-profile S1
switch(config)# dwrr queue 0 weight 5
switch(config)# dwrr queue 1 weight 10
switch(config)# dwrr queue 2 weight 15
switch(config)# dwrr queue 3 weight 20
switch(config)# dwrr queue 4 weight 25
switch(config)# dwrr queue 5 weight 50
```

The following commands illustrate an invalid configuration because local priority 2 is not assigned to a queue:

```

switch(config)# qos cos-map 1 local-priority 1
switch(config)# qos queue-profile Q1
switch(config)# map queue 0 local-priority 0
switch(config)# map queue 1 local-priority 1
switch(config)# map queue 3 local-priority 3
switch(config)# map queue 4 local-priority 4
switch(config)# map queue 5 local-priority 5
switch(config)# map queue 5 local-priority 6
switch(config)# map queue 5 local-priority 7
switch(config)# qos schedule-profile S1
switch(config)# dwrr queue 0 weight 5
switch(config)# dwrr queue 1 weight 10
switch(config)# dwrr queue 3 weight 15
switch(config)# dwrr queue 4 weight 25
switch(config)# dwrr queue 5 weight 50

```

Applying the QoS profile **Q1** and the schedule profile **S1** to all interfaces that do not have an applied interface-specific schedule profile:

```

switch(config)# apply qos queue-profile Q1 schedule-profile S1

```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config config-if config-lag-if	Administrators or local user group members with execution rights for this command.

apply qos threshold-profile



Only supported on the 8325, 9300, and 10000 Switch Series.

```

apply qos threshold-profile <THRESHOLD-NAME>
no apply qos threshold-profile

```

Description

Applies a threshold profile globally to all Ethernet and LAG interfaces on the switch, or to a specific interface. When applied globally, the specified threshold profile is configured only on Ethernet interfaces and LAGs that do not already have their own schedule profile.

The same profile can be applied both globally and locally to an interface. This guarantees that an interface always uses the specified threshold profile, even if the global profile is changed.

The **no** form of this command removes the specified threshold profile from an interface, and causes it to use the global threshold profile. This is the only way to remove a threshold profile override from an interface. A profile can only be deleted once it is no longer applied to any interface.

Parameter	Description
<code><THRESHOLD-NAME></code>	Specifies the name of the threshold profile to apply. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Example

Applying the threshold profile **mythreshold** to all interfaces that do not have an applied profile:

```
switch(config)# apply qos threshold-profile mythreshold
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config config-if config-lag-if	Administrators or local user group members with execution rights for this command.

clear queue-monitor interface

```
clear queue-monitor interface [<IFNAME>|<IFRANGE>]
```

Description

Clear the data collected on an interface since enabling queue monitoring. If no interfaces are specified, perform a clear of data collected on all interfaces with queue monitoring enabled.

Parameter	Description
<code><IFNAME></code>	Name of the interface. Format: <MEMBER>/<SLOT>/<PORT>
<code><IFRANGE></code>	Range of interfaces. Format: <MEMBER>/<SLOT>/<PORT>-<MEMBER>/<SLOT>/<PORT>

Examples

Clearing queue monitor data collected on interface 1/1/1:

```
config)# clear queue-monitor interface 1/1/1
Warning: clearing collected queue monitor statistics will be reflected
in all CLI sessions, any agents running in the analytics engine, and any
external systems monitoring switch statistics.
Continue (y/n)? y
```

Clearing queue monitor data collected on interfaces 1/1/1 and 1/1/2:

```
config)# clear queue-monitor interface 1/1/1-1/1/2
Warning: clearing collected queue monitor statistics will be reflected
in all CLI sessions, any agents running in the analytics engine, and any
external systems monitoring switch statistics.
Continue (y/n)? y
```

Clearing all queue monitor data collected on all interfaces:

```
config)# clear queue-monitor interface
Warning: clearing collected queue monitor statistics will be reflected
in all CLI sessions, any agents running in the analytics engine, and any
external systems monitoring switch statistics.
Continue (y/n)? y
```

Related Commands

Command	Description
queue-monitor	This command enables the queue monitoring feature, allowing the switch to collect queue statistics at 10-second time intervals. These aggregate statistics can be used to monitor network health, troubleshoot network issues, and identify normal network behavior patterns and performance anomalies. This feature is disabled by default, but can be enabled on a maximum of 52 interfaces per switch.



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced on 8100, 8325, 8325H, 8325P, 8360, 9300, 9300S and 10000 Switch series

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

dwrr queue

```
dwrr queue <QUEUE-NUMBER> weight <WEIGHT> [max-bandwidth <RATE> {kbps|percent} [burst <SIZE>]]
no dwrr queue <QUEUE-NUMBER> [weight <WEIGHT> [max-bandwidth <RATE> {kbps|percent} [burst <SIZE>]]
```

Description

Assigns the deficit weighted round robin (DWRR) algorithm and its weight to a queue in a schedule profile. DWRR allocates available bandwidth among all non-empty queues in relation to the queue weights.

Egress queue shaping can be configured using the **max-bandwidth** option to limit the amount of traffic transmitted per output queue at all times, even when there is leftover bandwidth available on the port. The buffer associated with each egress queue stores the excess traffic to smooth the output rate. Sustained rates of traffic above the maximum bandwidth will eventually fill the output queue, causing tail drops. Use **show interface <IF-NAME> queues** to determine if any tail-drop errors have occurred.

Use **show qos schedule-profile <NAME>** to view the settings of a specific schedule profile.

To remove only egress queue shaping, re-enter the dwrr queue command without the **max-bandwidth** parameter.

The **no** form of this command removes the DWRR algorithm from a queue in a schedule profile.

Parameter	Description
<QUEUE-NUMBER>	Specifies the queue number. Range: 0 to 7.
weight <WEIGHT>	Specifies the scheduling weight. Range: 1 to 127.
max-bandwidth <RATE>	Specifies the maximum bandwidth rate allowed on the queue in kbps. Range: 64 to 100000000. Alternatively, the maximum bandwidth rate can be configured on the queue as a percentage of the port shape or link bandwidth if a port shape is not configured. The allowed range is 1-100.

Examples

Assigning DWRR with a weight of **17** to queue **2** in the schedule profile **MySchedule**:

```
switch(config)# qos schedule-profile MySchedule
switch(config-schedule)# dwrr queue 2 weight 17
```

Deleting DWRR for queue **2** from the schedule profile **MySchedule**:

```
switch(config)# qos schedule-profile MySchedule
switch(config-schedule)# no dwrr queue 2
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.13	Added max-bandwidth and burst parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-schedule-<NAME>	Administrators or local user group members with execution rights for this command.

flow-control buffer cable-length

```
flow-control buffer cable-length {auto|<VALUE>}  
no flow-control buffer cable-length {auto|<VALUE>}
```

Description

Configures the cable length value in meters used to calculate the headroom buffer size if an explicit headroom buffer limit is not configured and flow-control is enabled. If auto is used then the L1 reported cable length is used to calculate the headroom buffer size.

If no headroom limit or cable length configuration is specified (or cable-length auto is specified but hardware is not reporting a cable length) then a default cable length of 350 meters is used to compute the headroom limit.

The **no** form of this command removes the existing cable length configuration.

Parameter	Description
auto	Specifies the interface-detected cable length.
<VALUE>	Specifies cable length value in meters.

Examples

Configuring a cable length of **400** meters on interface **1/1/1**:

```
switch(config)# interface 1/1/1  
switch(config-if)# flow-control buffer cable-length 400
```

Removing the configured cable length value of **400** meters on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer cable-length 400
```

Configuring interface-detected cable length on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer cable-length auto
```

Removing the configuration for interface-detected cable length on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer cable-length auto
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

map queue

```
map queue <QUEUE-NUMBER> local-priority <PRIORITY-NUMBER>
no map queue <QUEUE-NUMBER> [local-priority <PRIORITY-NUMBER>]
```

Description

Assigns a local priority to a queue in a queue profile. By default, the larger the queue number the higher its priority. A queue without a local priority value assigned to it is not used to store packets. The same queue can be assigned multiple local priorities.

The **no** form of this command removes the specified local priority from a specific queue. If no local priority number is specified, then all local priorities are removed from the queue.

Parameter	Description
<QUEUE-NUMBER>	Specifies the queue number. Range: 0 to 7.
<PRIORITY-NUMBER>	Specifies the local priority. Range: 0 to 7, where 0 is the lowest priority and 7 is the highest.

Usage

For a queue profile to be complete and ready to be applied, all eight local priorities must be mapped to a queue. Any local priority used by interface Priority-based Flow Control (PFC) must be the only local priority mapped to its queue. In order for PFC pausing to work as intended, no other local priorities should be mapped to that same queue. This queue mapping should be configured during initial switch provisioning and only changed during maintenance periods where all ports are disabled.



NOTE: PFC is only supported on the 8325, 9300, and 10000 Series Switch

The following commands illustrate a valid configuration, where every local priority value is assigned to a queue:

```
map queue 0 local-priority 0
map queue 1 local-priority 1
map queue 1 local-priority 2
map queue 3 local-priority 3
map queue 4 local-priority 4
map queue 5 local-priority 5
map queue 5 local-priority 6
map queue 5 local-priority 7
```

The following commands illustrate an invalid configuration, because local priority 2 is not assigned to a queue:

```
map queue 0 local-priority 0
map queue 1 local-priority 1
map queue 2 local-priority 3
map queue 3 local-priority 4
map queue 4 local-priority 5
map queue 5 local-priority 6
map queue 5 local-priority 7
```

Examples

Assigning priority **7** to queue **7** in profile **myprofile**:

```
switch(config)# qos queue-profile myprofile
switch(config-queue)# map queue 7 local-priority 7
```

Removing priority **7** from queue **7** in profile **myprofile**:

```
switch(config)# qos queue-profile myprofile
switch(config-queue)# no map queue 7 local-priority 7
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-queue	Administrators or local user group members with execution rights for this command.

name queue

```
name queue <QUEUE-NUMBER> <DESCRIPTION>
no name queue <QUEUE-NUMBER>
```

Description

Assigns a description to a queue in a queue profile. This is for identification purposes and has no effect on configuration.

The **no** form of this command removes the description associated with a queue.

Parameter	Description
<QUEUE-NUMBER>	Specifies the queue number. Range: 0 to 7.
<DESCRIPTION>	Specifies a queue description for identification purposes. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Examples

Assigning the description **priority-traffic** to queue **7**:

```
switch(config)# qos queue-profile myprofile
switch(config-queue)# name queue 7 priority-traffic
```

Removing the description from queue **7**:

```
switch(config)# qos queue-profile myprofile
switch(config-queue)# no name queue 7
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-queue	Administrators or local user group members with execution rights for this command.

qos cos-map

```
qos cos-map <CODE-POINT> local-priority <PRIORITY-NUMBER> [color <COLOR>] [name <DESCRIPTION>]
no qos cos-map <CODE-POINT>
```

Description

Defines the local priority assigned to incoming packets for a specific 802.1 VLAN priority code point (CoS) value. The CoS map values are used to mark incoming packets when QoS trust mode is set to **cos**. In **trust none** mode, CoS map entry 0 is used to set the port default local priority and color.

To see the default CoS map settings, use the following command:

```
switch# show qos cos-map default
code_point local_priority color name
-----
0          1             green Best_Effort
1          0             green Background
2          2             green Excellent_Effort
3          3             green Critical_Applications
4          4             green Video
5          5             green Voice
6          6             green Internetwork_Control
7          7             green Network_Control
```

The **no** form of this command restores the assignments for a CoS map value to the default setting.

Parameter	Description
<CODE-POINT>	Specifies an 802.1 VLAN priority CoS value. Range: 0 to 7. Default 0.
local-priority <PRIORITY-NUMBER>	Specifies a local priority value to associate with the CODE-POINT value. Range: 0 to 7. Default: 0.
color <COLOR>	Reserved for future use.
name <DESCRIPTION>	Specifies a description for the CoS setting. The name is for identification only, and has no effect on queue configuration. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Usage

Any code point configured for use by interface Priority-based Flow Control (PFC) must be assigned a unique local priority in the CoS map. No other code point can be assigned that same local priority. This should be configured during initial switch provisioning and only changed during maintenance periods where all ports are disabled.



NOTE: PFC is only supported on the 8325, 9300, and 10000 Series Switch

Examples

Mapping CoS value **1** to a local priority of **2**:

```
switch(config)# qos cos-map 1 local-priority 2
```

Mapping CoS value **1** to the default local priority value:

```
switch(config)# no qos cos-map 1
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

qos counters ecn

```
qos counters ecn  
no qos counters ecn
```

Description

Programs egress TCAM with entries that match on IP ECT (ECN-capable transport) fields including ECT(0) and ECT(1) as well as CE (congestion experienced) traffic and counts the matched packets.

Use the **show running-config** and **show interface <IFNAME> qos counters** commands to see the to see the status of the current **qos counters ecn** configuration.

The **no** form of the command will stop the egress TCAM from matching and counting packets with IP ECT fields.

Examples

Configuring Tx counters on interface **1/1/1** to match and count packets with IP ECT/CE fields:

```
switch(config)# interface 1/1/1  
switch(config-if)# qos counters ecn
```

Unconfiguring Tx counters on interface **1/1/1** to match and count packets with IP ECT/CE fields:

```
switch(config)# interface 1/1/1  
switch(config-if)# no qos counters ecn
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config-if	Administrators or local user group members with execution rights for this command.
9300S	config-lag-if	

qos counters rocev2

```
qos counters rocev2  
no qos counters rocev2
```

Description

Configures the ingress TCAM with entries that match fields which classify RoCEv2 CNP, NAK, Other, Total ACK, and Total RoCEv2 traffic and counts the matched packets.

Use the **show running-config** and **show interface <IF-NAME> qos counters** commands to see the status of the **qos counters rocev2** configuration.

The **no** form of this command will stop the ingress TCAM from matching and counting packets with RoCEv2 fields.

Examples

Configuring Rx counters on interface **1/1/1** to match and count packets with RoCEv2 fields:

```
switch(config)# interface 1/1/1  
switch(config-if)# qos counters rocev2
```

Unconfiguring Rx counters on interface **1/1/1** to match and count packets with RoCEv2 fields:

```
switch(config)# interface 1/1/1  
switch(config-if)# no qos counters rocev2
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

qos dscp

```
qos dscp <CODE-POINT>
no qos dscp
```

Description

Configures a differentiated services code point (DSCP) remark for an Ethernet or LAG interface. IPV4 and IPV6 packets that ingress on the interface are remarked at egress using the configured DSCP value.

The remark only occurs when QoS trust mode on the interface is set to **none**. If a DSCP remark is configured and then trust mode is subsequently set to **cos** or **dscp**, then the DSCP remark is ignored.

The following commands will show the remark status as *not applied* (incompatible QoS global or port trust configuration):

- **show running-configuration**
- **show interface <INTERFACE-NAME>**
- **show interface <INTERFACE-NAME> qos**

The **no** form of this command removes a CoS remark on an interface.

Parameter	Description
<CODE-POINT>	Specifies an IP differentiated services code point value. Range: 0 to 63.

Usage

Order of operation for arriving IPv4 or IPv6 packets:

1. Trust none is applied with initial local-priority and color metadata assigned from the CoS Map entry index 0.
2. The local-priority value and the queue profile are then used to determine the queue for the packet.

3. The remark of the packet's DSCP metadata field is performed. When the packet is transmitted, its IPv4 or IPv6 DS header is remarked with the DSCP metadata.

For arriving non-IP packets:

Trust none is applied with initial local-priority and color metadata assigned from the CoS Map entry index 0. This selects the queue for packet scheduling. The PCP of any tagged non-IP packets is unchanged.

Examples

Configuring a DSCP remark of **43** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# qos trust none
switch(config-if)# qos dscp 43
```

Deleting a DSCP remark of **43** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no dscp 43
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

qos dscp-map

```
qos dscp-map <CODE-POINT> local-priority <PRIORITY-NUMBER> [color <COLOR>] [name <DESCRIPTION>]
no qos dscp-map <CODE-POINT>
```

Description

Defines the local priority color assigned to incoming packets for a specific IP differentiated services code point (DSCP) value. The DSCP map values are used to prioritize incoming packets when QoS trust mode is set to **dscp**.

The **no** form of this command restores the assignments for a code point to the default setting.

Use **show qos dscp-map** to view the current settings. To see the default DSCP map settings, use the following command:

```

switch# show qos dscp-map default
code_point  local_priority  color    name
-----
0           1              green    CS0
1           1              green
2           1              green
3           1              green
4           1              green
5           1              green
...
45          5              green
46          5              green    EF
47          5              green
48          6              green    CS6
...
61          7              green
62          7              green
63          7              green

```

Parameter	Description
<code><CODE-POINT></code>	Specifies an IP differentiated services code point. Range: 0 to 63. Default: 0.
<code>local-priority <PRIORITY-NUMBER></code>	Specifies a local priority value to associate with the CODE-POINT value. Range: 0 to 7. Default: 0.
<code>color <COLOR></code>	Configures the QoS CoS map color. The supported colors are green, red, and yellow. The default color is green.
<code>cos <PCP-VALUE></code>	Specifies an optional 802.1p VLAN Priority Code Point remark value. Range: 0 to 7. Default: No remark.
<code>name <DESCRIPTION></code>	Specifies a description for the DSCP setting. The name is used for identification only, and has no effect on queue configuration. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Examples

Setting code point **1** to a local priority of **2** and a CoS of **0**:

```
switch(config)# qos dscp-map 1 local-priority 2 cos 0
```

Setting code point **1** to the default value:

```
switch(config)# no qos dscp-map 1
```

Setting code point **1, 3-5** to a local priority **2**, and CoS color as **green** with the description **EntryName**:

```
switch(config)# qos dscp-map 1,3-5 local-priority 2 color green name EntryName
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.13	Added <COLOR> parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

qos pool

```
qos pool <INDEX> lossless size {factory-default|<PERCENT>} percent headroom  
{factory-default|<HSIZE>} kbytes [priorities <PRIORITY>]  
no qos pool <INDEX> lossless size {factory-default|<PERCENT>} percent headroom  
{factory-default|<HSIZE>} kbytes [priorities <PRIORITY>]
```



It is not recommended to configure PFC on priority 7. This priority is used by protocol and control traffic, and device operation can be negatively impacted by pausing of traffic.

Description

Creates or modifies a packet buffer pool for lossless traffic by configuring lossless pool size, headroom buffer associated with the pool, and the priorities that are mapped to the pool.

The lossless pool size is a percentage of the total available buffer memory on the device. The headroom pool memory is allocated from the lossless pool and is used for storing packets that arrive on a port after pause has been asserted.

The **no** form of this command removes the QoS pool and returns the memory back to the default lossy pool.

Parameter	Description
<INDEX>	Specifies the index of the lossless pool.
factory-default	Specifies the default lossless pool or headroom buffer sizes.
<PERCENT>	Specifies the lossless pool size in percent. Default: 40.6. Range: 10 to 90.
<HSIZE>	Specifies the headroom buffer size in kilobytes. Factory-default

Parameter	Description
	size: 3072 kilobytes. Range: 0 to 10240 kilobytes or half the size of the lossless pool, whichever is lower.
<PRIORITY>	Specifies the PFC priorities to be mapped to the pool. Range: 0 to 7. To map multiple priorities, use a comma-separated list. Ex: 1,3,6.

Examples

Configuring the QoS pool using lossless pool size and headroom buffer size with one or two PFC assigned to it:

```
switch(config)# qos pool 1 lossless size 60 percent headroom 2048 kbytes
priorities 4
switch(config)# qos pool 1 lossless size 60 percent headroom 2048 kbytes
priorities 3,4
switch(config)# qos pool 1 lossless size factory-default percent headroom factory-
default kbytes priorities 3,4
```

Removing the QoS pool configuration:

```
switch(config)# no qos pool 1 lossless size 60 percent headroom 2048 kbytes
priorities 4
```

Removing a priority from the existing QoS pool configuration:

```
switch(config)# qos pool 2 lossless size 70 percent headroom 3072 kbytes
priorities 5,6
switch(config)# qos pool 2 lossless size 70 percent headroom 3072 kbytes
priorities 5
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.10.1000	Support for 9300 series switches added.
10.10	Support for 3 lossless pools added.
10.09	Support for 10000 series switches added.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

qos queue-profile

```
qos queue-profile <NAME>
no qos queue-profile <NAME>
```

Description

Creates a new QoS queue profile and switches to the **config-queue** context for the profile. Or, if the specified QoS queue profile exists, this command switches to the **config-queue** context for the profile. A queue profile maps queues to local-priority values. Each profile has one to eight queues numbered 0 to 7. The larger the queue number, the higher its priority during transmission scheduling.

The **no** form of this command removes the specified QoS queue profile. Only profiles that are not currently applied can be removed.

Parameter	Description
<NAME>	Specifies the name of the QoS queue profile to create or configure. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Examples

Creating the profile **myprofile**:

```
switch(config)# qos queue-profile myprofile
switch(config-queue)#
```

Deleting the profile **myprofile**:

```
switch(config)# no qos queue-profile myprofile
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

qos schedule-profile

```
qos schedule-profile <NAME>
no qos schedule-profile <NAME>
```

Description

Creates a QoS schedule profile and switches to the **config-schedule** context for the profile. If the specified schedule profile exists, this command switches to the **config-schedule** context for the profile. The schedule profile determines the order in which queues are selected to transmit a packet, and the amount of service defined for each queue.

Parameter	Description
<NAME>	Specifies the name of the QoS queue profile to create or configure. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Usage

Queues in a schedule profile are numbered consecutively starting from zero. Queue zero is the lowest priority queue. The larger the queue number, the higher priority the queue has in scheduling algorithms.

A profile named **factory-default** is defined by default and applied to all interfaces. It cannot be edited or deleted. To see its settings, use the command:

```
switch# show qos schedule-profile factory-default
queue_num algorithm weight
-----
0          dwrr       1
1          dwrr       1
2          dwrr       1
3          dwrr       1
4          dwrr       1
5          dwrr       1
6          dwrr       1
7          dwrr       1
```

A profile named **strict** is predefined and cannot be edited or deleted. The strict profile services all queues of the queue profile to which it is applied, using the strict priority algorithm.

A schedule profile must be defined on all interfaces at all times.

There are two permitted configurations for a schedule profile:

1. All queues use the same scheduling algorithm (for example, DWRR).
2. The highest queue number uses strict priority, and all remaining (lower) queues use the same algorithm (for example, DWRR). This supports priority scheduling behavior necessary for the IETF RFC 3246 Expedited Forwarding specification (<https://tools.ietf.org/html/rfc3246>).

Only limited changes can be made to an applied schedule profile:

- The weight of a dwrr queue.
- The bandwidth of a strict queue or a min-bandwidth queue.
- The algorithm of the highest numbered queue can be swapped between dwrr and strict, and vice versa.

Applicable to REST: Any other changes will result in an unusable schedule profile, and the switch will revert to the **factory-default** profile until the profile is corrected.

The **no** form of this command removes the specified QoS schedule profile when it is not applied. Only profiles that are not currently applied to an interface can be removed.

Examples

Creating the schedule profile **MySchedule**:

```
switch(config) # qos schedule-profile MySchedule
switch(config-schedule) #
```

Deleting the schedule profile **MySchedule**:

```
switch(config) # no qos schedule-profile MySchedule
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

qos shape

```
qos shape <RATE> [kbps|percent] [burst <SIZE>]
no qos shape
```

Description

Limits the egress bandwidth on an interface to a value that is lower than its line rate. An optional burst value may also be specified.

Errors will be generated in the following events:

- A user configures a port-shaping value that is greater than 100 percent
- A user configures a kbps port-shaping value that is less than the supported minimum kbps value. The supported minimum kbps shaping value can be retrieved using the **show capacities** command.

The **no** form of this command removes shaping from an interface.

Parameter	Description
<code><RATE></code>	Specifies the maximum traffic rate in kbps. Range: 1 to 400000000 for the HPE Aruba Networking 9300/9300S Switch Series. Alternatively, the bandwidth can also be configured as a percentage of link bandwidth. The supported range is 1-100. Default units are kilobits per second.
<code><SIZE></code>	Specifies the maximum burst size in kilobytes. Range: 1 to 128. Default: 32.

Usage

When the traffic rate destined for the port exceeds the configured egress bandwidth, the switch will buffer the excess up to the limit of the queues. Rates larger than the interface's link rate will have no effect. When set on a LAG, each member Ethernet port independently shapes its egress bandwidth to the specified rate.

Examples

Configuring an egress port shaping rate of 400 Mbps on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# qos shape 400000 kbps
```

Configuring an egress port-shaping rate of 40% on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# qos shape 40 percent
```

Deleting egress port shaping on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no qos shape
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

qos threshold-profile

```
qos threshold-profile <NAME>
no qos threshold-profile <NAME>
```

Description

Creates a QoS threshold profile and switches to the **config-threshold** context for the profile. If the specified threshold profile exists, this command switches to the **config-threshold** context for the existing profile. The threshold profile determines the action to take when a threshold is exceeded for each queue.

A threshold profile is composed of up to 8 queues, numbered from 0 to 7. Each queue defines the action to take when buffer utilization exceeds a specific threshold.

Configure queues with the command **queue**.

The **no** form of this command removes the specified QoS threshold profile. Only profiles that are not currently applied to an interface can be removed.

Parameter	Description
<NAME>	Specifies the name of the QoS threshold profile to create or configure. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).

Usage

Queues in a threshold profile can be any valid queue number, although it is also valid to create a threshold profile with no queues specified. Queue zero is the minimum allowed queue number. The maximum allowed queue number may vary by product. For products supporting eight queues, the largest queue number is seven. If an applied threshold profile specifies configuration of a queue number that is not in use based on the configured queue profile, the threshold configuration of that unused queue is ignored.

Examples

Creating the threshold profile **mythreshold**:

```
switch(config)# qos threshold-profile mythreshold
switch(config-threshold)#
```

Deleting the threshold profile **MySchedule**:

```
switch(config)# no qos threshold-profile mythreshold
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

qos trust

```
qos trust none [local-priority <PRIORITY-NUMBER>] [color <COLOR>]  
no qos trust
```

Description

In the **config** context:

- This command sets the trust mode that is globally applied to all interfaces that do not have a trust mode configured.
- The **no** form of this command restores all interfaces that do not currently have a trust mode configured to the default setting.

In the **config-if** context:

- This command sets the trust mode override for a specific interface.
- The **no** form of this command clears a trust mode override. The interface then uses the global setting. This is the only way to remove a trust mode override.

Parameter	Description
none	Ignores all packet headers. Ingress packets are assigned the local priority and color values configured for CoS map entry 0. Default.

Example

Setting the global trust mode to **dscp**, which is applied to all interfaces that do not already have an individual trust mode configured. An override is then applied to interface **2/2/2**, and LAG 100, setting trust mode to **cos**:

```
switch(config)# qos trust dscp  
switch(config)# interface 2/2/2  
switch(config-if)# qos trust cos  
switch(config-if)# interface lag 100  
switch(config-if)# qos trust cos
```



Note: The warning message *QoS port remark configurations are not applied when the QoS trust mode is cos or dscp*, is seen if a port trust command other than *trust none* is attempted when there is already a remark configuration on the port. To restore the old remark configuration, configure the port trust mode to *none*.



Note: The warning message *QoS port remark configurations are not applied when the global QoS trust mode is cos or dscp*, is seen if a port *no qos trust* command is attempted when there is already a remark configuration on the port and the global trust mode is not *none*. To re-apply the remark configuration, set the port trust mode to *none*.



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config config-if config-lag-if	Administrators or local user group members with execution rights for this command.

queue action

WRED

HPE Aruba Networking 8320, 8325, 8325P, 8325H, 9300/9300S, 9300S, 10000 Switch Series

```
queue <0-7> action wred-resp { green | yellow | red } min-threshold <WRED-MIN-LIMIT>
kbytes max-threshold <WRED-MAX-LIMIT> kbytes max-prob <WRED-MAX-PROB> percent
queue <0-7> action wred-non-resp { green | yellow | red } min-threshold <WRED-MIN-LIMIT>
kbytes max-threshold <WRED-MAX-LIMIT> kbytes max-prob <WRED-MAX-PROB> percent
```

ECN

HPE Aruba Networking 8325, 8325H, 8325P, 9300/9300S, 10000 Switch Series

```
queue <0-7> action ecn all threshold <LIMIT> kbytes
queue <0-7> action ecn all min-threshold <MIN-LIMIT> kbytes max-threshold <MAX-LIMIT>
kbytes
no queue <0-7>
```

Description

Defines the threshold settings and action for a specified queue in a threshold-profile. For ECN, when queue utilization exceeds the threshold value, ECT (ECN-Capable Transport) packets will be CE (Congestion Encountered) marked when transmitted.

For WRED, when queue utilization exceeds the threshold value, WRED action will randomly early-drop packets to signal congestion. More than one WRED action can be configured on a single queue for different packet colors.

When supported, dual threshold configures an ECN action based on the following queue thresholds:

- When the queue exceeds the minimum threshold limit, the ECN action marks ECT packets CE with increasing probability.
- When the queue exceeds the maximum threshold limit, the ECN action marks all ECT packets CE.

The **no** form of this command removes the settings for a queue.

Parameter	Description
<code><0-7></code>	Specifies the queue number. Range: 0 to 7.
<code><LIMIT>, <MIN-LIMIT>, <MAX-LIMIT></code>	Specifies the threshold value in kilobytes. Range: 0 to 6000 kilobytes.
<code><WRED-MIN-LIMIT></code>	Specifies the queue minimum utilization threshold value for WRED to probabilistically start dropping packets.
<code><WRED-MAX-LIMIT></code>	Specifies the queue maximum utilization threshold value for WRED, after which every packet is dropped.
<code><WRED-MAX-PROB></code>	Specifies the maximum WRED probability of dropping a packet for the specified queue. NOTE: Applicable only on the HPE Aruba Networking 6400v2, 8100, 8360v2, 8320, 8325, 8400, 9300/9300S, and 10000 Switch Series.

Examples

Assigning a threshold to queue **7** in profile **mythreshold**:

```
switch(config)# qos threshold-profile mythreshold
switch(config-threshold)# queue 7 action ecn all threshold 4000 kbytes
```

Assigning a minimum and maximum threshold in kilobytes to queue **5** in profile **mythreshold**:

```
switch(config)# qos threshold-profile mythreshold
switch(config-threshold)# queue 5 action ecn min-threshold 2000 kbytes max-
threshold 4000 kbytes
```

Configuring a responsive WRED action on queue 2 for red-, yellow-, and green-colored packets:

```
switch(config)# qos threshold-profile threshprofile
switch(config-threshold)# queue 2 action wred-resp green min-threshold 100 kbytes
max-threshold 2000 kbytes max-prob 70 percent
switch(config-threshold)# queue 2 action wred-resp yellow min-threshold 80 kbytes
max-threshold 1000 kbytes max-prob 85 percent
switch(config-threshold)# queue 2 action wred-resp red min-threshold 50 kbytes
max-threshold 900 kbytes max-prob 90 percent
```

Configuring a non-responsive WRED action on queue 4 for red-, yellow-, and green-colored packets:

```
switch(config)# qos threshold-profile threshprofile
switch(config-threshold)# queue 4 action wred-non-resp green min-threshold 500
kbytes max-threshold 2100 kbytes max-prob 71 percent
switch(config-threshold)# queue 4 action wred-non-resp yellow min-threshold 250
kbytes max-threshold 1000 kbytes max-prob 82 percent
switch(config-threshold)# queue 4 action wred-non-resp red min-threshold 50 kbytes
max-threshold 900 kbytes max-prob 95 percent
```

Removing a threshold from queue 7 in profile **mythreshold**:

```
switch(config)# qos threshold-profile mythreshold
switch(config-threshold)# no queue 7
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.11	WRED syntax support introduced in 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-threshold	Administrators or local user group members with execution rights for this command.

queue-monitor

```
queue-monitor
no queue-monitor
```

Description

This command enables the queue monitoring feature, allowing the switch to collect queue statistics. then display this information as a queue statistics history. These aggregate statistics can be used to monitor network health, troubleshoot network issues, and identify normal network behavior patterns

and performance anomalies. This feature is disabled by default, but can be enabled on a maximum of 52 interfaces per switch.

Examples

Enabling the queue monitoring feature on interface 1/1/1:

```
(config)# interface 1/1/1
(config-if)# queue-monitor
```

Disabling the queue monitoring feature on interface 1/1/1:

```
(config)# interface 1/1/1
(config-if)# no queue-monitor
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Related Commands

Command	Description
show queue-monitor status	This command is used to view the global state of the queue monitor feature. Output includes the memory consumed by the feature, the statistics being monitored for collection, and the interfaces currently enabled for monitoring.

Command History

Release	Modification
10.14.1000	Command introduced on 9300 Switch series

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

queue-monitor polling-interval seconds

```
queue-monitor polling-interval seconds <SEC>
no queue-monitor polling-interval seconds <SEC>
```

Description

Configures the polling interval used to sample interface queue data. The specified interval is applied to all interfaces where queue monitoring is enabled. Changing the polling interval clears all previously collected queue statistics and restarts data collection from the time the new interval is applied.

The **no** form of the command resets the polling interval to the default value of 10 seconds.

Parameter	Description
<code>polling-interval seconds <SEC></code>	Specifies the polling interval in seconds. Valid polling intervals are 1, 5, 10, 30, or 60 seconds.

Examples

Setting the polling interval to **1** second:

```
switch(config)# queue-monitor polling-interval seconds 1
```

Changing the polling interval while queue monitoring is enabled on one or more interfaces:

```
switch(config)# queue-monitor polling-interval seconds 20
Warning: changing the polling interval will clear collected queue monitor
statistics and will be reflected in all CLI sessions, any agents running in the
analytics engine, and any external systems monitoring switch statistics.

Continue (y/n)? y
```

Resetting the polling interval to the default of **10** seconds when no interfaces have queue monitoring enabled:

```
switch(config)# no queue-monitor polling-interval
```

Resetting the polling interval to the default of **10** seconds when one or more interfaces have queue monitoring enabled:

```
switch(config)# no queue-monitor polling-interval
Warning: changing the polling interval will clear collected queue monitor
statistics and will be reflected in all CLI sessions, any agents running in the
analytics engine, and any external systems monitoring switch statistics.

Continue (y/n)? y
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	<code>config</code>	Administrators or local user group members with execution rights for this command.

rate-limit

```
rate-limit {broadcast|multicast|unknown-unicast} <RATE> {percent|pps}  
no rate-limit {broadcast|multicast|unknown-unicast}
```

Description

Sets the amount of traffic of a specific type that can ingress on an Ethernet port, or on each port of a LAG interface. Rate limits are enforced separately on each individual member of a LAG, not on the LAG as a whole.

The HPE Aruba Networking 832x, 9300, and 10000 Switch Series do not allow mixing percentage-based and pps-based rate limits on the same interface at the same time. While the CLI prevents this, REST users who notice unapplied rate limits should check message logs to determine whether the failure is due to invalid configuration.

If an interface's overall rate-limiting configuration becomes invalid, any prior rate-limit settings remain in hardware until explicitly removed. This is to prevent unexpected excess traffic, in the event of accidental misconfiguration. Apart from deletions, other rate-limiting configuration changes on that interface are ignored until conflicts between the hardware unit-types are resolved (i.e., until all of the interface's rate-limit settings use only one of the two unit-types).

The **no** form of this command removes the traffic limit for the specified traffic type.

Parameter	Description
{broadcast multicast unknown-unicast}	Specifies the type of ingress traffic to which the rate limit applies: broadcast , multicast , or unknown-unicast . The multicast rate limit affects multicast and broadcast traffic. The broadcast rate limit only affects broadcast traffic. When both types are applied to the same interface, broadcast packets are limited to the lower of the two rate values. Layer 2 BPDU packets, like spanning tree, are also included in the multicast rate limit.
<RATE> {percent pps}	Specifies the rate limit in packets per second or as a percentage of link bandwidth. Range: 64 to 209090910 pps, or 1-100 percent. For percent mode, the actual rate limit will be approximately equivalent to the minimum of the two 64-kbps step values that are closest to the kbps-converted percentage rate. The actual applied rate limit can be verified using the show interface <IF-NAME> qos command. For percentage mode, rate-limits may be shown as "not applied" until after link-up has occurred on the configured port or LAG.



The HPE Aruba Networking 9300/9300S Switch Series has a range of 64 to 836363640 pps, or 1-100 percent.

Examples

Limiting **multicast** traffic to **4000 pps** on interface **1/1/3**:

```
switch(config)# interface 1/1/3  
switch(config-if)# rate-limit multicast 4000 pps
```

Viewing the results of the configuration setting:

```

switch# show interface 1/1/3 qos
Interface 1/3/3 is down (Administratively down)
Admin state is down
Hardware: Ethernet, MAC Address: 1c:98:ec:e3:6a:00
MTU 1500
Full-duplex
rate-limit multicast 4000 pps (4000 actual)

Speed 0 Mb/s
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
RX
    0 input packets          0 bytes
    0 input error            0 dropped
    0 CRC/FCS
L3:
    ucast: 0 packets, 0 bytes
    mcast: 0 packets, 0 bytes
TX
    0 output packets         0 bytes
    0 input error            0 dropped
    0 collision
L3:
    ucast: 0 packets, 0 bytes
    mcast: 0 packets, 0 bytes

```

Limiting **broadcast** traffic to **50 pps** on LAG 100:

```

switch# config
switch(config)# interface 1/1/3
switch(config-if)# interface lag 100
switch(config-if)# rate-limit broadcast 50 pps

```

Configuring an unknown-unicast rate-limit in packets per second:

```

switch(config)# interface 1/1/3
switch(config-if)# rate-limit unknown-unicast 100 pps

```

Configuring a multicast rate-limit as a percentage of link bandwidth:

```

switch(config)# interface 1/1/4
switch(config-if)# rate-limit multicast 1 percent

```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.13	Added the percent parameter.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

show interface queues

show interface <INTERFACE-NAME> queues

Description

Displays interface-level queue statistics.

Parameter	Description
<INTERFACE-NAME>	Specifies the name of an Ethernet port or LAG on the switch. Format: member/slot/port or lag number .

Usage

Statistics include:

- **Tx Bytes:** Total bytes transmitted. The byte count may include packet headers and internal metadata that are removed before the packet is transmitted. Packet headers added when the packet is transmitted may not be included.
- **Tx Packets:** Total packets transmitted.
- **Tx Drops:** Total packets dropped by an egress queue due to insufficient capacity.

Examples

Showing queue statistics for interface **1/1/5**:

```
switch# show interface 1/1/5 queues
Interface 1/1/5 is down
Admin state is up
      Tx Bytes      Tx Packets      Tx Drops
Q0              0             0             3
Q1          15356             73             0
Q2              0             0             0
Q3              0             0             0
Q4              0             0             0
Q5              0             0             0
Q6              0             0             0
Q7              0             0             0
```

Showing queue statistics for interface **lag 1**:

```
switch# show interface lag 1 queues
Aggregate-name lag1
Aggregated-interfaces :
1/1/6 1/1/7
Speed 20000 Mb/s
```

	Tx Bytes	Tx Packets	Tx Drops
Q0	0	0	0
Q1	0	0	0
Q2	0	0	0
Q3	0	0	0
Q4	0	0	0
Q5	0	0	0
Q6	0	0	0
Q7	3450	25	0



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface queue-monitor

```
show interface {<IFNAME>} queue-monitor
  histogram [filter [since <1-10000> days|hours|minutes|seconds] [type {queue-
    depth}|queue-tx-rate]
  list [filter [since <1-10000> days|hours|minutes|seconds] [threshold {kbps <1-
    4294967295>}|{kbytes <1-4294967295>}|{packets <1-4294967295>}} [type {queue-depth
    |queue-tx-rate}] [slot <slot-id>]
  table [filter [threshold {kbps <1-4294967295>}|{kbytes <1-4294967295>}|{packets <1-
    4294967295>}} [type {queue-depth}|queue-tx-rate}]
```

Description

Display queue statistics history in the CLI as either a list or a histogram, or as a table, showing the previous five minutes of queue statistics history.



This feature must be enabled on each interface.

Parameter	Description
interface [<IFNAME>]	Specifies the name of an Ethernet port or LAG on the switch. If the optional <IFNAME> parameter is omitted, the output of this command displays all queue statistic

Parameter	Description
	data for all interfaces. Format: <MEMBER>/<SLOT>/<PORT> or lag <ID>
histogram list table	Specifies the output format for queue monitor output. ■ histogram - Queue statistics history is presented in histogram format for the last 8 hours. ■ list - Queue statistics history is presented in the list format for the last 8 hours ■ table - Queue statistics history is presented in tabular format for the last 5 minutes.
filter	The list format is able to display all of the collected queue statistics history data when no filters are applied. To limit the information displayed in the output of this command, use the filter parameters to filter the output to the format and data you require.
since <1-10000> days hours minutes seconds	Show events no older than a specified age, measured in seconds, days, hours or minutes.
type {queue-depth} queue-tx-rate	Filter queue monitoring data by the specified filter type. If you do not specify a filter type, the type defaults to queue-depth . To see filtered output for other statistics types, you must specify the type. ■ queue-depth: Show queue depth data. ■ queue-tx-rate: Show average queue transmission (tx) rate data.
threshold {kbps kbytes packets <1-4294967295>}	Show data that exceeds a specified threshold in kilobytes, number of packets, or kilobits per second.

Examples

Displaying the queue statistics history data for all monitored interfaces in list format:

```
switch# show interface queue-monitor list
Time Range: 8 hours (2023-08-07 09:11:30 to 2023-08-08 17:11:30 (UTC+00:00))
```

Time	Interface	Queue	Statistic	Value
2023-08-08 17:11:10	1/1/9	4	Average Queue Tx Rate	54321 kbps
2023-08-08 17:11:20	1/1/8	4	Average Queue Tx Rate	1234 kbps
2023-08-08 17:11:20	1/1/9	4	Average Queue Tx Rate	54321 kbps
2023-08-08 17:11:30	1/1/8	4	Average Queue Tx Rate	1234 kbps
2023-08-08 17:11:30	1/1/9	4	Average Queue Tx Rate	54321 kbps

The following example displays a portion of output of the **show interface 1/1/8 queue-monitor** command, showing queue statistics history data in tabular format for interface 1/1/8 with a min-depth of 2 kbytes.

```

switch# show interface 1/1/8 queue-monitor table min-depth kbytes 2
1/1/8 Statistics History
Collection Interval: 10 seconds
Time Range: 2023-08-08 17:07:00 to 2023-08-08 17:12:00 (UTC)
Min-Depth Filter: 2 KB

```

Time (s)	Queue Depth - bytes							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
-300	-	-	-	-	-	-	-	-
-295	-	-	-	-	-	-	-	-
-290	-	-	-	-	-	-	-	-
-285	-	-	-	-	-	-	-	-
-280	-	-	-	-	-	-	-	-
-275	-	-	-	-	-	-	-	-
-270	-	-	-	-	-	-	-	-
-265	-	-	-	-	-	-	-	-
-260	-	-	-	-	-	-	-	-
-255	-	-	-	-	-	-	-	-
-250	-	2078	-	-	-	-	-	-
-245	-	9914	-	-	-	-	-	-
-240	-	171102	-	-	-	-	-	-
-235	-	996262	-	-	-	-	-	-
-230	-	5444	-	-	-	-	-	-
-225	-	-	-	-	-	-	-	-
-220	-	-	-	-	-	-	-	-
-215	-	-	-	-	-	-	-	-
-210	-	-	-	-	-	-	-	-
-205	-	-	-	-	-	-	-	-
-200	-	-	-	-	-	-	-	-
...								

Displaying the queue statistics history data for interface 1/1/8 in histogram format.

```

switch(config)# show interface 1/1/8 queue-monitor histogram
1/1/8 Statistics History
Time Range: 2023-08-08 09:12:15 to 2023-08-08 17:12:15 (UTC)
Samples per Queue: 13

```

Depth (KB)	Count at Depth							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
0	13	13	13	13	7	13	13	10
1-64	0	0	0	0	6	0	0	3
65-128	0	0	0	0	0	0	0	0
129-256	0	0	0	0	0	0	0	0
257-512	0	0	0	0	0	0	0	0
513-1024	0	0	0	0	0	0	0	0
1025-2048	0	0	0	0	0	0	0	0
2049-4096	0	0	0	0	0	0	0	0
4097-8192	0	0	0	0	0	0	0	0
8193-16384	0	0	0	0	0	0	0	0
16385-32768	0	0	0	0	0	0	0	0
32769-65536	0	0	0	0	0	0	0	0

Output of the global **show** command when queue monitoring is not enabled on any interfaces.

```

switch(config)# show interface queue-monitor list
Queue monitoring is not enabled on any interfaces.

```

Output of the **show** command when the interface requested does not have queue monitoring enabled.

```
switch(config)# show interface 1/1/8 queue-monitor table  
Interface 1/1/8 does not have queue monitoring enabled.
```

Output of the global **show** command with the list presentation specified when there is no relevant data to show. Note: the table and histogram presentation formats output all enabled interface data.

```
switch(config)# show interface queue-monitor list  
Enabled interfaces have not collected any data.
```

Output of the **show** command for an interface with the list presentation specified but there is no relevant data to show.

```
switch(config)# show interface 1/1/8 queue-monitor list  
Interface 1/1/8 has not collected any data.
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Related Commands

Command	Description
queue-monitor	This command enables the queue monitoring feature, allowing the switch to collect queue statistics at 10-second time intervals. These aggregate statistics can be used to monitor network health, troubleshoot network issues, and identify normal network behavior patterns and performance anomalies. This feature is disabled by default, but can be enabled on a maximum of 52 interfaces per switch.

Command History

Release	Modification
10.14.1000	Command introduced on 9300 and 9300S Switch series

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface queue-monitor status

```
show interface {<IFNAME> | <IFRANGE>} queue-monitor status [vsx-peer]
```

Description

Displays the queue monitoring status for a specific interface or range of interfaces. If no interface is specified, the command will display the queue monitoring status for all interfaces configured.

Parameter	Description
{<IFNAME> <IFRANGE>}	Use the queue-monitor status parameters to show whether the feature is enabled or disabled, and information about memory consumption and monitored interfaces. Include the optional <IFNAME> parameter to filter the output of this command to show data for just the specified interface, or include both the <IFNAME> parameter and the additional <IFRANGE> parameter also to view data for a range of interfaces. If no interface is specified, the command will display the queue monitor status for all interfaces that have queue monitoring configured.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing queue monitoring status for interface **1/1/1** when queue monitoring is not configured on that interface.

```
switch# show interface 1/1/1 queue-monitor status
Interface 1/1/1 does not have queue monitoring enabled.
```

Showing the queue monitoring status for interface **1/1/1** when queue monitoring is enabled on that interface.

```
switch# show interface 1/1/1 queue-monitor status
Interface 1/1/1

Status                : Enabled
Monitored Statistics : , queue-tx-rate
```

Showing the queue monitoring status for a range of interfaces when queue monitoring is enabled on those interfaces.

```
switch# show interface 1/1/1-1/1/2 queue-monitor status
Interface 1/1/1

Status                : Enabled
Monitored Statistics : , queue-tx-rate

Interface 1/1/2

Status                : Enabled
Monitored Statistics : , queue-tx-rate
```

Showing the queue monitoring status for all interfaces that have queue monitoring enabled, but the interface does not support any statistics.

```
switch# show interface queue-monitor status
Interface 1/1/1

Status                : Blocked (No queue statistics supported for monitoring)

Interface 1/1/2

Status                : Blocked (No queue statistics supported for monitoring)

Interface 1/1/3 does not have queue monitoring enabled.
```

Showing the queue monitoring status for all interfaces where queue monitoring is enabled on interface **1/1/1**.

```
switch# show interface queue-monitor status
Interface 1/1/1

Status                : Enabled
Monitored Statistics  : , queue-tx-rate

Interface 1/1/2 does not have queue monitoring enabled.

Interface 1/1/3 does not have queue monitoring enabled.
```

Showing the queue monitoring status for all interfaces when the feature pack is invalid and queue monitoring is configured only on interface **1/1/1**.

```
switch# show interface queue-monitor status
Interface 1/1/1

Status                : Blocked (Invalid feature pack)

Interface 1/1/2 does not have queue monitoring enabled.

Interface 1/1/3 does not have queue monitoring enabled.
```

Showing the queue monitoring status for interface **1/1/1** when the feature pack is invalid and queue monitoring is configured on that interface.

```
switch# show interface 1/1/1 queue-monitor status
Interface 1/1/1

Status                : Blocked (Invalid feature pack)
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface qos

show interface <INTERFACE-NAME> qos

Description

Shows various QoS settings for a specific interface.

Parameter	Description
<INTERFACE-NAME>	Specifies the name of an interface on the switch. Format: member/slot/port or lag number .

Examples

Showing QoS settings for interface **1/1/5**:

```
switch# show interface 1/1/5 qos
Interface 1/1/5 is down
Admin state is up
qos trust none (global)
qos queue-profile factory-default (global)
qos schedule-profile EQSExample (override)
qos dscp 47
rate-limit unknown-unicast 64 pps (64 actual)
rate-limit broadcast 500 pps (500 actual)
qos shape 200000 kbps (200064 kbps actual) burst 70 (70 actual)
```

Queue	Maximum Bandwidth	Bandwidth Units	Burst (KB)
Q1	10082461	kbps	120
Q4	20164923	kbps	32
Q7	30247384	kbps	120

Showing QoS settings for interface **1/1/6**:



The following example applies only to the HPE Aruba Networking 8320, 8325, and 1000 Switch Series.

```
switch# show interface 1/1/6 qos
Interface 1/1/6 is down
Admin state is up
qos trust none (global)
qos queue-profile factory-default (global)
qos schedule-profile EQSExample (override)
rate-limit multicast 1 percent (100000 actual)
qos shape 200000 kbps (200064 kbps actual) burst 70 (70 actual)
```

Maximum	Bandwidth	Burst

Queue	Bandwidth	Units	(KB)
Q1	10082461	kbps	120
Q4	20164923	kbps	32
Q7	30247384	kbps	120

Showing QoS settings for interface **1/1/6**:



The following example applies only to the HPE Aruba Networking 9300 Switch Series.

```
switch# show interface 1/1/6 qos
Interface 1/1/6 is down
Admin state is up
qos trust none (global)
qos queue-profile factory-default (global)
qos schedule-profile EQSExample (override)
rate-limit multicast 1 percent (400000 actual)
qos shape 200000 kbps (200064 kbps actual) burst 70 (70 actual)
```

Queue	Maximum Bandwidth	Bandwidth Units	Burst (KB)
Q1	10082461	kbps	120
Q4	20164923	kbps	32
Q7	30247384	kbps	120



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface qos buffers

show interface <INTERFACE-NAME> qos buffers

Description

Shows interface-level buffer usage statistics.

Parameter	Description
<INTERFACE-NAME>	Specifies the name of an Ethernet port on the switch.

Usage

Usage statistics include:

- **In-Use:** Current buffer memory consumption in kilobytes for each priority.
- **Recent-Peak:** Maximum amount of buffer memory consumed by each priority since the last time the statistics were queried.
- **Max-Use:** Maximum amount of buffer memory consumed by each priority since the statistics were last cleared.
- **Limit:** Specifies the hardware-programmed usage limit for the row. Priorities configured for lossless behavior display two rows:
 - First row displays lossless pool usage and configured XOFF limit.
 - Second row displays headroom pool usage and the configured limit.

The hardware-programmed headroom pool limit is based on configuration of either the **flow-control buffer headroom** or **flow-control buffer cable-length** commands on the interface. If both configurations are specified on the same interface, the headroom buffer limit configuration takes precedence over the cable length. If auto is configured, then the hardware interface detected cable-length is used. If no headroom limit or cable length configuration is specified (or cable-length auto is specified but hardware is not reporting a cable length) then a default cable length of 350 meters is used to compute the headroom limit.

Examples

Showing buffer statistics for interface **1/1/1**:

```
switch# show interface 1/1/1 qos buffers
Buffer usage for 1/1/1 in kbytes:

Cable Length: 350 meters (default)
Recent Peak Interval: 50 seconds
Dynamic thresholds limit = 2^<Alpha>*FreeSpace
```

Ingress:

Pri	Pool type	Pool Id	In Use	Recent Peak	Max Use	Limit
---	-----	-----	-----	-----	-----	-----
0	Lossy	0	1486	2357	4852	
1	Lossless	1	542	1468	5123	Dyn:1
1	Headroom	1	0	0	6	65
2	Lossless	2	4825	7658	12240	Dyn:1
2	Headroom	2	0	0	0	65
3	Lossy	0	0	0	0	
4	Lossy	0	0	0	0	
5	Lossy	0	0	0	0	
6	Lossy	0	0	0	0	
7	Lossy	0	0	0	0	

Showing buffer statistics for interface **1/1/2**:


```
switch# show interface 1/1/2 qos buffers
Buffer usage for 1/1/2 in kbytes:

Cable Length: 400 meters (user configured)
Recent Peak Interval: 50 seconds
Dynamic thresholds limit = 2^<Alpha>*FreeSpace
```

Ingress:

Pri	Pool type	Pool Id	In Use	Recent Peak	Max Use	Limit
---	-----	-----	-----	-----	-----	-----
0	Lossy	0	1486	2357	4852	
1	Lossless	1	542	1468	5123	Dyn:1
1	Headroom	1	0	0	6	66
2	Lossless	2	4825	7658	12240	Dyn:1
2	Headroom	2	0	0	0	66
3	Lossy	0	0	0	0	
4	Lossy	0	0	0	0	
5	Lossy	0	0	0	0	
6	Lossy	0	0	0	0	
7	Lossy	0	0	0	0	

Showing buffer statistics for interface **1/1/3**:

```
switch# show interface 1/1/3 qos buffers
Buffer usage for 1/1/3 in kbytes:

Cable Length: 50 meters (hardware detected)
Recent Peak Interval: 50 seconds
Dynamic thresholds limit = 2^<Alpha>*FreeSpace
```

Ingress:

Pri	Pool type	Pool Id	In Use	Recent Peak	Max Use	Limit
---	-----	-----	-----	-----	-----	-----
0	Lossy	0	1486	2357	4852	
1	Lossless	1	542	1468	5123	Dyn:1
1	Headroom	1	0	0	6	55
2	Lossless	2	4825	7658	12240	Dyn:1
2	Headroom	2	0	0	0	55
3	Lossy	0	0	0	0	
4	Lossy	0	0	0	0	
5	Lossy	0	0	0	0	
6	Lossy	0	0	0	0	
7	Lossy	0	0	0	0	



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface qos counters

show interface <INTERFACE-NAME> qos counters

Description

Shows interface-level RoCEv2 and ECN counters.

Parameter	Description
<INTERFACE-NAME>	Specifies the name of an Ethernet port on the switch.

Examples

Showing qos counter statistics for interface **1/1/1**:

```
switch# show int 1/1/1 qos counters

Configured hardware counters for 1/1/1:

RoCEv2 Counters: Enabled
ECN Counters: Enabled
-----
Counter                               Value
-----
RoCEv2 RX Packet Counters:
  CNP                                10
  ACK                                30
  Other                             1840
  Total                             1900

ECN TX Packet Counters:
  ECT                                1100
  CE                                 700
```

Showing qos counter statistics for interface **1/1/1** when counters are not enabled in TCAM:

```
switch# show interface 1/1/1 qos counters

Configured hardware counters for 1/1/1:

RoCEv2 Counters: Disabled
ECN Counters: Disabled
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.16.1000	Command introduced.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos cos-map

`show qos cos-map [default] [vsx-peer]`

Description

Shows the global QoS CoS code point settings, or the factory default settings.

Parameter	Description
default	Shows the factory default CoS code point settings.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the current CoS map:

```
switch# show qos cos-map
code_point local_priority color name
-----
0          2             green Best_Effort
1          0             green Background
2          1             green Spare
3          3             green Excellent_Effort
4          4             green Controlled_Load
5          5             green Video
6          6             green Voice
7          7             green Network_Control
```

Showing the default CoS map:

```
switch# show qos cos-map default
code_point local_priority color name
-----
0          1             green Best_Effort
1          0             green Background
2          2             green Excellent_Effort
3          3             green Critical_Applications
4          4             green Video
```

5	5	green	Voice
6	6	green	Internetwork_Control
7	7	green	Network_Control



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos dscp-map

```
show qos dscp-map [default] [vsx-peer]
```

Description

Displays the current or default global QoS dscp-map.

Parameter	Description
default	Shows the factory default DSCP code point settings.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the current QoS DSCP map:

```
switch# show qos dscp-map
code_point local_priority color  name
-----
0          1              green  CS0
1          1              green
2          1              green
3          1              green
4          1              green
5          1              green
```

6	1	green	
7	1	green	
8	0	green	CS1
...			
45	5	green	
46	7	green	EF
47	5	green	
48	6	green	CS6
...			
61	7	green	
62	7	green	
63	7	green	

Showing the default QoS DSCP map:

```
switch# show qos dscp-map default
code_point local_priority color name
-----
0          1             green CS0
1          1             green
2          1             green
3          1             green
4          1             green
5          1             green
...
45         5             green
46         5             green EF
47         5             green
48         6             green CS6
...
61         7             green
62         7             green
63         7             green
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos pool

show qos pool [config [vsx-peer] | statistics]

Description

Shows the QoS pool buffer configuration and analysis information.

Parameter	Description
config	Shows the current pool configuration.
statistics	Shows the pool statistics.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the QoS global pool configuration and analysis:

```
switch# show qos pool

Global Packet-Buffer Overview (in Kbytes)

Packet Buffer Pools      Size      Port Limits      Max Usage
-----
Lossy Pool               4105      --               3242
Lossless Pool 1          13080 (50.00%) --               9235
  Headroom Pool 1        2058      --               0
    Sum of port headroom limits --         198           --
Lossless Pool 2          8973 (37.10%) --               8467
  Headroom Pool 2        2058      --               974
    Sum of port headroom limits --         265           --
-----
TOTAL:                   32768

Analysis:
Lossy Pool      was 79% utilized
Lossless pool 1 was 71% utilized
Headroom pool 1 is 90% over-provisioned
Lossless pool 2 was 94% utilized
Headroom pool 2 is 87% over-provisioned

...
```

Showing the QoS current pool configuration:

```
switch# show qos pool config

Global Packet-Buffer Configuration (in Kbytes)

Packet Buffer Pools      Size      Port Limits
-----
Lossy Pool               4105      --
Lossless Pool 1          13080 (50.00%) --
```

```

Headroom Pool 1                2058      --
Sum of port headroom limits      --      198

Lossless Pool 2                8973 (37.10%)  --
Headroom Pool 2                2058      --
Sum of port headroom limits      --      265
-----
TOTAL:                          32768

Lossless Pool 1                XOFF  Headroom
-----
1/1/1 priority 3                Dynamic 2      49
1/1/4 priority 3                Dynamic 2      49
1/1/50:1-1/1/50:2 priority 3   Dynamic 2      50
-----
TOTAL:                          --      198

Lossless Pool 2                XOFF  Headroom
-----
1/1/4 priority 5                Dynamic 2      49
1/1/16 priority 5              Dynamic 2      24
1/1/32-1/1/33 priority 5       Dynamic 2      96
-----
TOTAL:                          --      265
...

```

Showing the QoS pool statistics:

```

switch# show qos pool statistics

Packet-Buffer Pool Statistics

Recent-Peak Interval: 37 seconds

Packet Buffer Pools    Total Size    Peak Use    Recent Peak    Current Use
-----
Lossy Pool             6144         4852         2357           1486
Lossless Pool 1        10240        5123         1468           542
  Headroom 1           2048          6            0              0
Lossless Pool 2        12280       12240        7658          4825
  Headroom 2           2048          0            0              0

All buffer sizes are in Kbytes.
...

```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release

Modification

10.10.1000

Support for 9300 series switches added.

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos queue-profile

```
show qos queue-profile [<NAME> | factory-default] [vsx-peer]
```

Description

Shows the status of all queue profiles, or a specific queue profile.

Parameter	Description
<NAME>	Specifies the name of a queue profile. Range 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).
[factory-default]	Specifies the factory default queue profile.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

The status of a queue profile can be:

- Applied - The profile is actively being used by the switch.
- Complete - The profile meets the criteria to be applied.
- Incomplete - The profile does not meet the criteria to be applied.

For a queue profile to be complete and ready to be applied:

- All eight local priorities must be mapped to some queue.
- There can be 1 to 8 queues.

Examples

Showing the settings of the factory default queue profile:

```
switch# show qos queue-profile factory-default
queue_num local_priorities name
-----
0          0
1          1
2          2
3          3
4          4
5          5
6          6
7          7
```




For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos schedule-profile

```
show qos schedule-profile [<NAME> | factory-default | strict] [vsx-peer]
```

Description

Shows the status of all schedule profiles, or a specific schedule profile.

Parameter	Description
<NAME>	Specifies the name of a queue or schedule profile. Range: 1 to 64 alphanumeric characters, including period (.), underscore (_), and hyphen (-).
[factory-default]	Specifies the factory default queue profile.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

The status of a schedule profile can be:

- Applied - The profile is actively being used by one or more ports.
- Complete - The profile meets the criteria to be applied.
- Incomplete - The profile does not meet the criteria to be applied.

For a schedule profile to be complete and ready to be applied it must have:

- An algorithm for each queue defined by the applied queue profile.
- All queues must use the same algorithm except for the highest numbered queue, which may be strict.

Example

Showing the status of all schedule profiles:

```
switch# show qos schedule-profile
profile_status profile_name
-----
applied        MySchedule
complete       factory-default
complete       Test
```

Showing the configuration of factory default schedule profile:

```
switch# show qos schedule-profile factory-default
Queue
Number  Algorithm      Weight
-----
0        dwrr            1
1        dwrr            1
2        dwrr            1
3        dwrr            1
4        dwrr            1
5        dwrr            1
6        dwrr            1
7        dwrr            1
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos threshold-profile

```
show qos threshold-profile [<NAME>] [vsx-peer]
```

Description

Shows the status of all threshold profiles, or a specific threshold profile.

Parameter	Description
<NAME>	Specifies the name of a threshold profile. Range: 1 to 64

Parameter	Description
	alphanumeric characters, including period (.), underscore (_), and hyphen (-).
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Status fields are:

- applied: The threshold profile is applied to all configured ports.
- partially applied: The threshold profile is applied to some configured ports but failed on other configured ports.
- not applied: The threshold profile could not be applied to any configured ports.
- blank field: The threshold profile is not applied in the configuration (globally or as a port override).

Examples

Showing the status of threshold profile **mythreshold**:

On the 8325, 9300, and 10000 switches:

```
switch# show qos threshold-profile mythreshold
```

Queue	Action	Color	Minimum	Maximum	Max Probability
2	wred-resp	green	1000	1200	30
2	wred-non-resp	red	1100	1150	40
3	ecn	all	1200	1300	

Port	Status
1/1/1	applied
1/1/8	applied
1/2/2	applied

On the 8100 and 8360 switches:

```
switch# show qos threshold-profile mythreshold
```

queue_num	action	Threshold
5	ecn	40
7	ecn	50

Ports	Status
1/1/1	applied
1/1/8	applied
1/2/2	applied



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.08	Updated the example.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show qos trust

show qos trust [default] [vsx-peer]

Description

Shows the global QoS trust settings, or the factory default settings.

Parameter	Description
default	Shows the factory default QoS trust settings.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the current QoS trust settings:

```
switch# show qos trust
qos trust cos
```

Showing the default QoS trust settings:

```
switch# show qos trust default
qos trust none
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show queue-monitor status

`show queue-monitor status`

Description

Displays the global state of the queue monitoring feature. The output includes the global enable/disable status, the memory consumed by the feature, the statistics being collected, and the interfaces currently enabled for monitoring.

Examples

Showing queue monitoring status when queue monitoring is not enabled on any interfaces.

```
switch# show queue-monitor status
Feature Status           : Running
Memory Consumption       : 0 kbytes
Monitored Interfaces/Max : 0/52
```

Showing the queue monitoring status when queue monitoring is enabled on interface **1/1/1**.

```
switch# show queue-monitor status
Feature Status           : Running
Memory Consumption       : 184 kbytes
Polling Interval        : 10 seconds
Data Retention Duration  : 8 hours
Monitored Interfaces/Max : 1/52
Monitored Interfaces     : 1/1/1
```



For more information on features that use this command, refer to the Monitoring Guide for your switch model.

Related Commands

Command	Description
queue-monitor	This command enables the queue monitoring feature, allowing the switch to collect queue statistics at 10-second time intervals. These aggregate statistics can be used to monitor network health, troubleshoot network issues, and identify normal network

Command	Description
	behavior patterns and performance anomalies. This feature is disabled by default, but can be enabled on a maximum of 52 interfaces per switch.

Command History

Release	Modification
10.14.1000	Command introduced on 9300 and 9300S Switch series

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

strict queue

```
strict queue <0-7> [max-bandwidth <RATE> [kbps|percent]][burst <SIZE>]]
no strict queue <0-7> [max-bandwidth <RATE> [kbps|percent]][burst <SIZE>]]
```

Description

Assigns the strict priority algorithm to a queue. Strict priority services all packets waiting in a queue, before servicing the packets in lower priority queues.

Egress queue shaping can be configured using the **max-bandwidth** and **burst** options to limit the amount of traffic transmitted per output queue. The buffer associated with each egress queue stores the excess traffic to absorb bursts and smooth the output rate. Sustained rates of traffic above the maximum bandwidth will eventually fill the output queue, causing tail drops. Use **show interface <IF-NAME> queues** to determine if any tail-drop errors have occurred.

The **no** form of this command removes the the queue configuration from the schedule profile. To remove only egress queue shaping, re-enter the strict queue command without the **max-bandwidth** and **burst** parameters.

Parameter	Description
<QUEUE-NUMBER>	Specifies the number of the queue. Range: 0 to 7.
max-bandwidth <BANDWIDTH>	Specifies the maximum bandwidth allowed on the queue in Kbps. Range: 8 to 100000000. Alternatively, the maximum bandwidth rate can also be configured on the queue as a percentage of the port shape or link bandwidth if a port shape is not configured. The allowed range is 1-100.
burst <SIZE>	Specifies the maximum burst allowed on the queue. HPE Aruba Networking 8320, 8325 and 10000 Switch Series: Range: 1 to 1073. Default: 32. HPE Aruba Networking 9300 Switch Series: Range: 1 to 1024. Default: 32.

Parameter	Description
	HPE Aruba Networking 8400 Switch Series: Range: 1 to 32. Default: 32.

Usage

Either all the queues of the schedule profile can be *strict* or just the highest numbered queue. When applied to a LAG, each member Ethernet port independently schedules its egress transmissions using the strict settings. Only limited changes can be made to a *strict* queue that is part of an applied schedule profile:

- The max-bandwidth settings.
- The highest numbered queue can be swapped between *strict* and *dwrr*

Any other changes or removing a queue (**no strict queue**) will result in an unusable schedule profile. If that schedule profile is applied in the interface context, the switch will revert to the schedule profile applied in the global context until the profile is corrected. If that schedule profile is applied in the global context, the switch will revert to using the factory-default profile until the profile is corrected.

It is possible for the following errors to occur:

- **The max-bandwidth cannot be greater than 100 percent.**

This error occurs when a max-bandwidth value greater than 100 percent is configured on a queue.

- **The max-bandwidth cannot be less than <NUM> kbps.**

This error occurs when a kbps max-bandwidth value less than the supported minimum kbps shape value is configured on a queue. The supported minimum kbps shape value can be retrieved using the **show capacities** command.

Examples

Assigning strict priority to queue **7** in the schedule profile **MySchedule**:

```
switch(config)# qos schedule-profile MySchedule
switch(config-schedule)# strict queue 7
```

Deleting strict priority from queue **7** in the schedule profile **MySchedule**:

```
switch(config)# qos schedule-profile MySchedule
switch(config-schedule)# no strict queue 7
```

Assigning strict priority to queue **7** in the schedule profile **MySchedule** with a maximum bandwidth of 10000 Kbps and a burst of 62 Kbytes:

```
switch(config)# qos schedule-profile myschedule
switch(config-schedule)# strict queue 7 max-bandwidth 10000 kbps
```

Assigning strict priority to queue 7 in the schedule profile MySchedule with a maximum bandwidth of 40 percent and a burst of 62 Kbytes:

```
switch(config)# qos schedule-profile MySchedule
switch(config-schedule)# strict queue 7 max-bandwidth 40 percent
```



For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.13	Added the kbps and percent parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-schedule- <i><NAME></i>	Administrators or local user group members with execution rights for this command.

aaa accounting allow-fail-through

```
aaa accounting allow-fail-through
no aaa accounting allow-fail-through
```

Description

Enables accounting fail-through. When this option is enabled, the next server or accounting method is attempted after an accounting failure.

The **no** form of this command disables accounting fail-through. The system only attempts to reach the next server or accounting method if there is an accounting failure due to an unreachable TACACS+ or RADIUS server or a shared key mismatch error between the switch and the server.

Example

Enabling accounting fail-through:

```
switch(config)# aaa accounting allow-fail-through
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa accounting all-mgmt

```
aaa accounting all-mgmt <CONNECTION-TYPE> start-stop {local | group <GROUP-LIST>}
no aaa accounting all-mgmt <CONNECTION-TYPE> start-stop {local | group <GROUP-LIST>}
```

Description

Defines accounting as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for accounting purposes.

For remote accounting, the information is sent to the first reachable remote server that was configured with this command for remote accounting. If no remote server is reachable, local accounting remains available. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote accounting.



The system accounting log is not associated with any connection type (channel) and is therefore sent to the accounting method configured on the default connection type (channel) only.

The **no** form of this command removes for the specified connection type, any defined remote AAA server group accounting sequence. Local accounting is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<code><CONNECTION-TYPE></code>	One of these connection types (channels): default Defines a list of accounting server groups to be used for the default connection type. This configuration applies to all other connection types (console, ssh, https-server, telnet) that are not explicitly configured with this command. For example, if you do not use aaa accounting all-mgmt console... to define the console accounting list, then this default configuration is used for console. console Defines a list of accounting server groups to be used for the console connection type. ssh Defines a list of accounting server groups to be used for the ssh connection type. https-server Defines a list of accounting server groups to be used for the https-server (REST, Web UI) connection type. telnet Defines a list of accounting server groups to be used for the telnet connection type.
<code>start-stop</code>	Selects accounting information capture at both the beginning and end of a process.
<code>local</code>	Selects local-only accounting when used without the group parameter.
<code>group <GROUP-LIST></code>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa

Parameter	Description
	group server and servers are added to a server group with the command server. If the remote server(s) in the group is unreachable or if there is a key mismatch error between the switch and the AAA Server, then the next accounting method is attempted.

Usage

Local accounting is always active. It cannot be turned off.

Examples

Defining the default accounting sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local accounting.

```
switch(config)# aaa accounting all-mgmt default start-stop group tg1 tg2 tacacs
local
```

Defining the console accounting sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local accounting.

```
switch(config)# aaa accounting all-mgmt console start-stop group tg2 tg3 tacacs
local
```

Defining the ssh accounting sequence based on one user-defined TACACS+ server group and then the default TACACS+ server group.

```
switch(config)# aaa accounting all-mgmt ssh start-stop group tg2 tacacs
```

Defining the Telnet accounting sequence based on one user-defined TACACS+ server group and then the default TACACS+ server groups.

```
switch(config)# aaa accounting all-mgmt telnet start-stop group tg1 tacacs
```

Defining the default accounting sequence based on two user-defined RADIUS server groups, then the default RADIUS server group, and finally (if needed), local accounting.

```
switch(config)# aaa accounting all-mgmt default start-stop group rg1 rg2 radius
local
```

Defining the https-server accounting sequence based on one user-defined RADIUS server group and then the default RADIUS server group.

```
switch(config)# aaa accounting all-mgmt https-server start-stop group rg1 radius
```

Setting local accounting for the default connection type:

```
switch(config)# aaa accounting all-mgmt default start-stop local
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Added the telnet parameter for all other platforms.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication allow-fail-through

```
aaa authentication allow-fail-through  
no aaa authentication allow-fail-through
```

Description

Enables authentication fail-through. If this feature is enabled, the next server or authentication method is tried after an authentication failure.

The **no** form of this command disables authentication fail-through. The system only attempts to reach the next server or authentication method if there is an accounting failure due to an unreachable TACACS+/RADIUS server or a shared key mismatch error between the switch and the server.



If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Example

Enabling authentication fail-through:

```
switch(config)# aaa authentication allow-fail-through
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authentication login

```
aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}
no aaa authentication login <CONNECTION-TYPE> {local | group <GROUP-LIST>}
```

Description

Defines authentication as being local (with the name **local**) (the default). Or defines a sequence of remote AAA server groups to be accessed for authentication purposes. Each available connection type (channel) can be configured individually as either local or using remote AAA server groups. All server groups named in your command, must exist. This command can be issued multiple times, once for each connection type. Local is always available for any connection type not configured for remote AAA authentication.



If you do not want local authentication to occur in cases where all AAA servers contacted reject the user's credentials, do not enable authentication fail-through (command **aaa authentication allow-fail-through**).

The **no** form of this command removes for the specified connection type, any defined remote AAA server group authentication sequence. Local authentication is available for connection types without a configured remote AAA server group list (whether default or for the specific connection type).

Parameter	Description
<code><CONNECTION-TYPE></code>	One of these connection types (channels): default Defines a list of AAA server groups to be used for the default connection type. This configuration applies to all other connection types (console, ssh, https-server, telnet) that are not explicitly configured with this command. For example, if you do not use aaa accounting all-mgmt console... to define the console accounting list, then this default configuration is used for console. console Defines a list of AAA server groups to be used for the console connection type. ssh Defines a list of AAA server groups to be used for the ssh connection type. https-server Defines a list of AAA server groups to be used for the https-server (REST, Web UI) connection type.

Parameter	Description
	telnet Defines a list of AAA server groups to be used for the telnet connection type.
local	Selects local-only authentication when used without the group parameter.
group <GROUP-LIST>	Specifies the list of remote AAA server group names. Each name can be specified one time. Predefined remote AAA group names tacacs and radius are available. Although not a group name, predefined name local is available. User-defined TACACS+ and RADIUS server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa group server and servers are added to a server group with the command server . If the remote server(s) in the group is unreachable or if there is a key mismatch error between switch and the AAA Server, then the next authentication method is attempted.

Examples

Defining the default authentication sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local authentication.

```
switch(config)# aaa authentication login default group tg1 tg2 tacacs local
```

Defining the default authentication sequence based on two user-defined TACACS+ server groups, then the default TACACS+ server group, and finally (if needed), local authentication.

```
switch(config)# aaa authentication login console group tg2 tg3 tacacs local
```

Defining the ssh authentication sequence based on one user-defined TACACS+ server group and then the default TACACS+ server group.

```
switch(config)# aaa authentication login ssh group tg2 tacacs
```

Defining the Telnet authentication sequence with two user-defined TACACS+ server groups, the default TACACS+ server group, and finally (if needed), local authentication.

```
switch(config)# switch(config)# aaa authentication login telnet group tg1 tg2 tacacs local
```

Defining the default authentication sequence based on two user-defined RADIUS server groups, then the default RADIUS server group, and finally (if needed), local authentication.

```
switch(config)# aaa authentication login default group rg1 rg2 radius local
```

Defining the https-server authentication sequence based on one user-defined RADIUS server group and then the default RADIUS server group.

```
switch(config)# aaa authentication login https-server group rg1 radius
```

Setting local authentication for the default connection type:

```
switch(config)# aaa authentication login default local
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Added the telnet parameter on 10000, 9300, 83xx, 6100, 6000 and 4100i Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authorization allow-fail-through

```
aaa authorization allow-fail-through  
no aaa authorization allow-fail-through
```

Description

Enables authorization fail-through. When this option is enabled, the next server or authorization method is attempted after an authorization failure.

The **no** form of this command disables authorization fail-through. The system only attempts to reach the next server or authorization method if there is an authorization failure due to an unreachable TACACS+ server or a shared key mismatch error between the switch and the server.



If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Example

Enabling authorization fail-through:

```
switch(config)# aaa authorization allow-fail-through
```

The following configurations use authorization fail-through in different scenarios.

Example configuration one:

```
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa group server tacacs CPPM-TACACS
server 172.16.1.12
aaa authentication login ssh group CPPM-TACACS local
aaa authorization commands ssh group CPPM-TACACS local
```

Example configuration one does not support authentication via the TACACS+ server for a locally configured user. If the user is configured locally and that user does not have a profile present in the TACACS+ server, authentication fails with TACACS+, but the user is authenticated successfully with local authentication. Similarly, if authorization is rejected, the user is authorized locally with a fail-through configuration.

Example configuration two:

```
aaa group server tacacs CPPM-TACACS
server 172.16.1.12
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa authentication login ssh group CPPM-TACACS local
aaa authorization commands ssh group local CPPM-TACACS
```

With configuration two, if a user's profile is configured only in the TACACS+ server, user authorization is rejected locally and is authorized with TACACS using the fail-through configuration. When authentication fail-through is configured, if the first authentication method fails, authentication is attempted using the next server or authentication method. The authorization fail-through is based on the authorization sequence, and is independent of the authentication method of the user.

Example configuration three:

```
aaa group server tacacs CPPM-TACACS
server 172.16.1.12
aaa group server tacacs TACACS
server 192.168.10.15
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa authentication login ssh group CPPM-TACACS local
aaa authorization commands ssh group TACACS local
```

Example configuration four:

```
aaa group server radius RAD-GRP
server 172.16.1.12
aaa group server tacacs TACACS
server 192.168.10.15
aaa authentication allow-fail-through
aaa authorization allow-fail-through
aaa authentication login ssh group RAD-GRP local
aaa authorization commands ssh group TACACS local
```

With configurations three and four, the **CPPM-TACACS** or **RAD-GRP** groups reject authentication requests for locally configured users, and the users are authenticated locally with fail-through.

Authorization is attempted with the TACACS group in these configurations, and if this authorization attempt fails, the user will be authorized locally due to the fail-through configuration.



When authorization is rejected by multiple servers/server groups due to the fail-through configuration, a delay may be seen while executing commands.



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.12.1000	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa authorization commands

```
aaa authorization commands <CONNECTION-TYPE> {local | none}
no aaa authorization commands <CONNECTION-TYPE> {local | none}
aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
no aaa authorization commands <CONNECTION-TYPE> group <GROUP-LIST>
```

Description

Defines authorization as being basic local RBAC (specified as **none**), or as full-fledged local RBAC specified as **local** (the default), or as remote TACACS+ (specified with group <GROUP-LIST>). Each available connection type (channel) can be configured individually. All server groups named in the command, must exist. This command can be issued multiple times, once for each connection type.

The **no** form of this command unconfigures authorization for the specified connection type, reverting to the default of **local**.



Although only TACACS+ servers are supported for remote authorization, local authorization (basic or full-fledged) can be used with remote RADIUS authentication. If your switch uses command authorization, best practices is to configure [authorization fail-through](#) before configuring authentication fail-through. If not, the switch may fall into an unusable state where authorization will fail for all commands.

Parameter	Description
<CONNECTION-TYPE>	One of these connection types (channels): default Selects the default connection type for configuration. This configuration applies to all other connection types (console , ssh , telnet) that are not explicitly configured with this

Parameter	Description
	command. For example, if you do not use aaa authorization commands console... to define the console authorization list, then this default configuration is used for console. console Selects the console connection type for configuration. ssh Selects the ssh connection type for configuration. telnet Selects the telnet connection type for configuration.
local	When used alone without group <i><GROUP-LIST></i>, selects local authorization which can be used to provide authorization for a purely local setup without any remote AAA servers and also for when RADIUS is used for remote Authentication and Accounting but Authorization is local. When used after group, provides for fallback (to full-fledged local authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: If any TACACS+ server in the specified groups is reachable, but the command fails to be authorized by that server, the command is rejected and local authorization is never attempted. Local authorization is only attempted if every TACACS+ server cannot be reached.
none	When used alone without group <i><GROUP-LIST></i>, selects basic local RBAC authorization, for use with the built-in user groups (administrators, operators, auditors). When used after group, provides for fallback (to basic local RBAC authorization) when every server in every specified TACACS+ server group cannot be reached. NOTE: With none, for users belonging to user-defined user groups, all commands can be executed regardless of what authorization rules are defined in such groups. For per-command local authorization, use local instead.
group <i><GROUP-LIST></i>	Specifies the list of remote AAA server group names. Predefined remote AAA group name tacacs is available. User-defined TACACS+ server group names may also be used. The remote AAA server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command aaa server group and servers are added to a server group using command server. It is recommended to always include either the special name local or none as the last name in the group list. If both local and none are omitted, and no remote AAA server is reachable (or the first reachable server cannot authorize the command), command execution for the current user will not be possible. If the AAA server(s) in the group are not reachable, or if there is a key mismatch error between the server and the switch, the next authorization method is attempted.

Usage

TACACS+ server authorization considerations



Use caution when configuring authorization, as it has no fail through. If the switch is not configured properly, the switch might get into an unusable state in which all command execution is prohibited.

To prevent authorization difficulties:

- Make sure that all listed TACACS+ servers can authorize users for command execution.
- Make sure that credential database changes are promptly synchronized across all TACACS+ servers.
- Make sure either **local** or **none** is included as the last name in the group list. If both **local** and **none** are omitted, and no remote TACACS+ server is reachable (or the first reachable server cannot authorize), authorization will not be possible.
- Although not recommended, if you choose to omit both **local** and **none** from the list, and are manipulating configuration files, special caution is necessary. If the source configuration includes TACACS+ authorization and you are copying configuration from an existing switch into the running configuration of a new switch, and you have not yet configured the interface or routing information to reach the TACACS+ server, the switch will enter an unusable state, requiring hard reboot.
To avoid getting into this situation that can occur when **local** and **none** have been omitted, do either of the following:
 - In the configuration source, delete or comment-out the line configuring remote authorization. Then, after the configuration copy and paste, manually configure authorization.
 - Move the line configuring the authorization to the end of the source configuration before copying and pasting.

Examples

Defining the default authorization sequence based on a user-defined TACACS+ server group, then the default TACACS+ server group, and finally (as a precaution), **local** authorization:

```
switch(config)# aaa authorization commands default group tg1 tacacs local
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
```

Defining the Telnet authorization sequence based on a user-defined TACACS+ server group, then the default TACACS+ server group, and finally (as a precaution), **local** authorization:

```
switch(config)# aaa authorization commands telnet group tg1 tacacs local
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
```

Defining the console authorization sequence based on two user-defined TACACS+ server groups, and finally (as a precaution), **local** authorization:

```
switch(config)# aaa authorization commands console group tg1 tg2 local
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
```

Setting the authorization for default to **local**:

```
switch(config)# aaa authorization commands default local
```

Setting the authorization for the SSH interface to **none**:

```
switch(config)# aaa authorization commands ssh none
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11	Added the telnet parameter on the 10000, 9300, 83xx, 6100, 6000 and 4100i Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

aaa group server

```
aaa group server {tacacs | radius} <SERVER-GROUP-NAME>  
no aaa group server {tacacs | radius} <SERVER-GROUP-NAME>
```

Description

Creates an AAA server group that is either empty or contains preconfigured RADIUS/TACACS+ servers. You can create a maximum of 28 server groups.

The **no** form of this command deletes a server group. Only a preconfigured user-defined RADIUS/TACACS+ server group can be deleted. RADIUS or TACACS+ servers that were in a deleted server group remain a part of their default server group. The default server group for TACACS+ servers is **tacacs**. The default server group for RADIUS servers is **radius**.

Parameter	Description
server {tacacs radius}	Select either tacacs or radius for the server type.
<SERVER-GROUP-NAME>	Specifies the name of the server group to be created. The name of the server group can have a maximum of 32 characters.

Examples

Creating TACACS+ server group sg1:

```
switch(config)# aaa group server tacacs sg1
```

Creating RADIUS server group sg3:

```
switch(config)# aaa group server radius sg3
```

Deleting TACACS+ server group sg1:

```
switch(config)# no aaa group server tacacs sg1
```

Deleting RADIUS server group sg3:

```
switch(config)# no aaa group server radius sg3
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server auth-type

```
radius-server auth-type {pap | chap}  
no radius-server auth-type {pap | chap}
```

Description

Enables the CHAP or PAP authentication protocol, which is used for communication with the RADIUS servers, at the global level. You can override this command with a fine-grained per server **auth-type** configuration.

The **no** form of this command resets the global authentication mechanism for RADIUS to PAP or CHAP. PAP is the default authentication mechanism for RADIUS.

Parameter	Description
auth-type {pap chap}	Selects either the PAP or CHAP authentication protocol.

Examples

Authenticating CHAP:

```
switch(config)# radius-server auth-type chap
```

Authenticating PAP:

```
switch(config)# radius-server auth-type pap
```

Removing CHAP authentication:

```
switch(config)# no radius-server auth-type chap
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server host

```
radius-server host {<FQDN> | <IPv4> | <IPv6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}][vrf <VRF-NAME>]  
no radius-server host {<FQDN> | <IPv4> | <IPv6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}][vrf <VRF-NAME>]
```

Description

Adds a RADIUS server. By default, the RADIUS server is associated with the server group named **radius**. The **no** form of this command removes a previously added RADIUS server.



For enhanced security with IPsec, the alternative command **radius-server host secure ipsec** is available. The standard non-IPsec **radius-server host** command does not modify any existing IPsec configuration. If IPsec is already configured for the RADIUS server, then IPsec will remain enabled for the server.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as:

Parameter	Description
	▪ <code><FQDN></code>: a fully qualified domain name. ▪ <code><IPv4></code>: an IPv4 address. ▪ <code><IPv6></code>: an IPv6 address.
<code>key [plaintext <PASSKEY> </code> <code> ciphertext <PASSKEY>]</code>	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 128 alphanumeric and special characters. NOTE: When key is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the key parameter without entering other parameters. The entered passkey characters are masked with asterisks. When key is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command radius-server key is available for setting the global passkey.
<code>timeout <TIMEOUT-SECONDS></code>	Specifies the timeout. Range: 1 to 60 seconds. If a timeout is not specified, the value from the global timeout for RADIUS is used.
<code>port <PORT-NUMBER></code>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
<code>auth-type {pap chap}</code>	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the RADIUS global default is used.
<code>acct-port <ACCT-PORT></code>	Specifies the UDP accounting port number. Range: 1 to 65535. Default: 1813.
<code>retries <RETRY-COUNT></code>	Specifies the number of retry attempts for contacting the specified RADIUS server. Range is 0 to 5 attempts. If no retry value is provided, the default value of 1 is used.
<code>tracking {enable disable}</code>	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command radius-server tracking to configure RADIUS server tracking globally. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.
<code>tracking-mode {any dead-only}</code>	Configures tracking mode for the RADIUS server that has tracking enabled with the server. The tracking mode is used to monitor the status of RADIUS server reachability. The default tracking mode is any. any Track the RADIUS server irrespective of its server reachability. dead-only

Parameter	Description
	Track the RADIUS server only when the server is marked as unreachable.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Usage

If the fully qualified domain name is provided for the RADIUS server, a DNS server must be configured and accessible through the same VRF which is configured for the RADIUS server. This configuration is required for the resolution of the RADIUS server hostname to its IP address. If a DNS server is not available for this VRF, the RADIUS servers reachable through this VRF must be configured by means of their IP addresses only.

Examples

Adding a RADIUS server with an IPv4 address and a prompted passkey:

```
switch(config)# radius-server host 1.1.1.5 key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
```

Deleting a RADIUS server with an IPv4 address and a prompted passkey:

```
switch(config)# no radius-server host 1.1.1.5 key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
```

Adding a RADIUS server with an IPv4 address and a named VRF:

```
switch(config)# radius-server host 1.1.1.1 vrf mgmt
```

Deleting a RADIUS server with an IPv4 address and a named VRF:

```
switch(config)# no radius-server host 1.1.1.1 vrf mgmt
```

Adding a RADIUS server with an IPv4 address, a port, and a named VRF:

```
switch(config)# radius-server host 1.1.1.2 port 32 vrf mgmt
```

Deleting a RADIUS server with an IPv4 address, a port, and a named VRF:

```
switch(config)# no radius-server host 1.1.1.2 port 32 vrf mgmt
```


Adding a RADIUS server with an FQDN, a timeout, port number, and a named VRF:

```
switch(config)# radius-server host abc.com timeout 15 port 32 vrf vrf_blue
```

Deleting a RADIUS server with an FQDN, a timeout, port number, and a named VRF:

```
switch(config)# no radius-server host abc.com timeout 15 port 32 vrf vrf_blue
```

Adding a RADIUS server with an IPv6 address:

```
switch(config)# radius-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Deleting a RADIUS server with an IPv6 address:

```
switch(config)# no radius-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Adding a RADIUS server with tracking enabled and tracking mode is set to dead-only:

```
switch(config)# radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
```

Deleting a RADIUS server with tracking enabled and tracking mode is set to dead-only:

```
switch(config)# no radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
```

Adding a RADIUS server with tracking disabled:

```
switch(config)# radius-server host 1.1.1.1 tracking disable
```

Deleting a RADIUS server with tracking disabled:

```
switch(config)# no radius-server host 1.1.1.1 tracking disable
```

Adding a RADIUS server with an IPv4 address, key, encrypted passkey, number of retries, and VRF name:

```
switch(config)# radius-server host 1.1.1.6 key ciphertext AQBapStbgHt1X2JlbcEcQ1  
xbbzWjrFr9UsfH3+00x5Qj0qcQBAAAAJ5WZBQ= retries 3 vrf vrf_red
```

Deleting a RADIUS server with an IPv4 address, key, encrypted passkey, number of retries, and VRF name:

```
switch(config)# no radius-server host 1.1.1.6 key ciphertext  
AQBapStbgHt1X2JlbcEcQ1  
xbbzWjrFr9UsfH3+00x5Qj0qcQBAAAAJ5WZBQ= retries 3 vrf vrf_red
```

Deleting a RADIUS server with an IPv4 address and specified VRF:

```
switch(config)# no radius-server host 1.1.1.1 vrf mgmt
```

Deleting a RADIUS server with an FQDN, port, and specified VRF:

```
switch(config)# no radius-server host abc.com port 32 vrf vrf_blue
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.17	The key length for the plaintext value in the key parameter has been increased from 32 to 128 characters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server host secure ipsec

Syntax for a RADIUS server that uses IPsec for authentication:

```
radius-server host {<FQDN> | <IPV4> | <IPV6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]  
    secure ipsec authentication spi <SPI-INDEX> <AUTH-TYPE> <AUTH-KEY-TYPE> [<AUTH-KEY>]  
no radius-server host {<FQDN> | <IPV4> | <IPV6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]  
    secure ipsec authentication spi <SPI-INDEX><AUTH-TYPE><AUTH-KEY-TYPE> [<AUTH-KEY>]
```

Syntax for a RADIUS server that uses IPsec for both authentication and encryption:

```
radius-server host {<FQDN> | <IPV4> | <IPV6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]  
    [tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]  
    secure ipsec encryption spi <SPI-INDEX> <AUTH-TYPE> <AUTH-KEY-TYPE>  
    [<AUTH-KEY>] <ENCRYPT-TYPE> <ENCRYPT-KEY-TYPE> [<ENCRYPT-KEY>]  
no radius-server host {<FQDN> | <IPV4> | <IPV6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
```

```
[timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]
[auth-type {pap | chap}] [acct-port <ACCT-PORT>] [retries <RETRY-COUNT>]
[tracking {enable | disable}] [tracking-mode {any | dead-only}] [vrf <VRF-NAME>]
secure ipsec encryption spi <SPI-INDEX><AUTH-TYPE><AUTH-KEY-TYPE>
[<AUTH-KEY>] <ENCRYPT-TYPE><ENCRYPT-KEY-TYPE> [<ENCRYPT-KEY>]
```

Description

Adds a RADIUS server that uses IPsec for enhanced security (authentication and possibly encryption). By default, the RADIUS server is associated with the server group named **radius**.

The **no** form of this command removes a previously added RADIUS (with IPsec) server.



Unless enhanced security with IPsec is required, use the **radius-server host** command instead.

Parameter	Description
{<FQDN> <IPV4> <IPV6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPV4>: an IPv4 address. ▪ <IPV6>: an IPv6 address.
key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 128 alphanumeric and special characters. NOTE: When key is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the key parameter without entering other parameters. The entered passkey characters are masked with asterisks. When key is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command radius-server key is available for setting the global passkey.
timeout <TIMEOUT-SECONDS>	Specifies the timeout. Range: 1 to 60 seconds. If a timeout is not specified, the value from the global timeout for RADIUS is used.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
auth-type {pap chap}	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the RADIUS global default is used.
acct-port <ACCT-PORT>	Specifies the UDP accounting port number. Range: 1 to 65535. Default: 1813.
retries <RETRY-COUNT>	Specifies the number of retry attempts for contacting the specified RADIUS server. Range is 0 to 5 attempts. If no retry value is provided, the default value of 1 is used.
tracking {enable disable}	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command radius-server tracking to configure RADIUS

Parameter	Description
	server tracking globally. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.
tracking-mode {any dead-only}	Configures tracking mode for the RADIUS server that has tracking enabled with the server. The tracking mode is used to monitor the status of RADIUS server reachability. The default tracking mode is any . any Track the RADIUS server irrespective of its server reachability. dead-only Track the RADIUS server only when the server is marked as unreachable.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.
spi <SPI-INDEX>	Specifies the Security Parameters Index. The SPI is an identification tag carried in the IPsec AH header. The SPI must be unique on the switch. Range: 256 to 4294967295.
<AUTH-TYPE>	Specifies the authentication algorithm: md5 , sha1 , or sha256 .
<AUTH-KEY-TYPE>	Specifies the authentication key type: plaintext , hex-string , or ciphertext .
[<AUTH-KEY>]	Specifies the authentication key. For <AUTH-TYPE> of ciphertext , this is the ciphertext string. For <AUTH-TYPE> of plaintext or hex-string : ▪ md5 (plaintext): 1 to 16 characters, (hex-string): 2 to 32 hexadecimal digits. ▪ sha1 (plaintext): 1 to 20 characters, (hex-string): 2 to 40 hexadecimal digits. ▪ sha256 (plaintext): 1 to 32 characters, (hex-string): 2 to 64 hexadecimal digits. NOTE: When <AUTH-KEY-TYPE> is not followed by <AUTH-KEY>, plaintext authentication key prompting occurs upon pressing Enter. Enter must be pressed immediately after the <AUTH-KEY-TYPE> parameter without entering other parameters. The entered authentication key characters are masked with asterisks.
<ENCRYPT-TYPE>	Specifies the encryption algorithm: 3des , aes , des , or null .
<ENCRYPT-KEY-TYPE>	Specifies the encryption key type: plaintext , hex-string , or ciphertext .
[<ENCRYPT-KEY>]	Specifies the encryption key. For <ENCRYPT-TYPE> of ciphertext , this is the ciphertext string.

Parameter	Description
	For <i><ENCRYPT-TYPE></i> of plaintext or hex-string: ▪ 3des (plaintext): 24 characters, (hex-string): 48 hexadecimal digits. ▪ aes (plaintext): 16, 24, or 32 characters, (hex-string): 32, 48, or 64 hexadecimal digits. ▪ des (plaintext): 8 characters, (hex-string): 16 hexadecimal digits. NOTE: When <i><ENCRYPT-KEY-TYPE></i> is not followed by <i><ENCRYPT-KEY></i>, plaintext encryption key prompting occurs upon pressing Enter. Enter must be pressed immediately after the <i><ENCRYPT-KEY-TYPE></i> parameter without entering other parameters. The entered encryption key characters are masked with asterisks.

Usage

If the fully qualified domain name is provided for the RADIUS server host, a DNS server must be configured and accessible through the same VRF as mentioned for the server host. This configuration is required for the resolution of the RADIUS server hostname to its IP address. If a DNS server is not available for this VRF, the RADIUS servers reachable through this VRF must be configured by means of their IP addresses only.

Examples

Adding a RADIUS server with an IPv4 address, a plaintext passkey, and IPsec authentication (md5 plaintext).

```
switch(config)# radius-server host 1.1.1.1 key plaintext 98ab vrf mgmt secure
ipsec authentication spi 261 md5 plaintext labc
```

Deleting a RADIUS server with an IPv4 address, a plaintext passkey, and IPsec authentication (md5 plaintext).

```
switch(config)# no radius-server host 1.1.1.1 key plaintext 98ab vrf mgmt secure
ipsec authentication spi 261 md5 plaintext labc
```

Adding a RADIUS server with an IPv4 address and a prompted IPsec authentication (md5) plaintext authentication key.

```
switch(config)# radius-server host 1.1.1.1 secure ipsec authentication spi 261
md5
Enter the IPsec authentication key: *****
Re-Enter the IPsec authentication key: *****
```

Deleting a RADIUS server with an IPv4 address and a prompted IPsec authentication (md5) plaintext authentication key.

```
switch(config)# no radius-server host 1.1.1.1 secure ipsec authentication spi 261 md5  
Enter the IPsec authentication key: *****  
Re-Enter the IPsec authentication key: *****
```

Adding a RADIUS server with an IPv4 address, IPsec authentication (MD5 plaintext), and IPsec encryption (AES plaintext):

```
switch(config)# radius-server host 1.1.1.2 vrf mgmt secure  
ipsec encryption spi 262 md5 plaintext 9xyz aes plaintext 1234567890abcdef
```

Deleting a RADIUS server with an IPv4 address, IPsec authentication (MD5 plaintext), and IPsec encryption (AES plaintext):

```
switch(config)# no radius-server host 1.1.1.2 vrf mgmt secure  
ipsec encryption spi 262 md5 plaintext 9xyz aes plaintext 1234567890abcdef
```

Adding a RADIUS server by providing an IPv4 address and IPsec MD5 authentication type, and then responding to prompts for the keys and encryption type:

```
switch(config)# radius-server host 1.1.1.6 secure ipsec encryption spi 262 md5  
Enter the IPsec authentication key: *****  
Re-Enter the IPsec authentication key: *****  
  
Enter the IPsec encryption type (3des/aes/des/null)? aes  
  
Enter the IPsec encryption key: *****  
Re-Enter the IPsec encryption key: *****
```

Deleting a RADIUS server by providing an IPv4 address and IPsec MD5 authentication type, and then responding to prompts for the keys and encryption type:

```
switch(config)# no radius-server host 1.1.1.6 secure ipsec encryption spi 262 md5  
Enter the IPsec authentication key: *****  
Re-Enter the IPsec authentication key: *****  
  
Enter the IPsec encryption type (3des/aes/des/null)? aes  
  
Enter the IPsec encryption key: *****  
Re-Enter the IPsec encryption key: *****
```

Adding a RADIUS server with an IPv4 address, tracking enabled, tracking mode, IPsec authentication (MD5 plaintext), IPsec encryption (AES plaintext) is set to dead-only:

```
switch(config)# radius-server host 1.1.1.1 tracking enable tracking-mode dead-only  
vrf mgmt secure ipsec encryption spi 262 md5 plaintext 9xyz  
aes plaintext 1234567890abcdef
```

Deleting a RADIUS server with an IPv4 address, tracking enabled, tracking mode, IPsec authentication (MD5 plaintext), IPsec encryption (AES plaintext) is set to dead-only:

```
switch(config)# no radius-server host 1.1.1.1 tracking enable tracking-mode dead-only
                vrf mgmt secure ipsec encryption spi 262 md5 plaintext 9xyz
                aes plaintext 1234567890abcdef
```

Removing a RADIUS server:

```
switch(config)# no radius-server host 1.1.1.1 vrf mgmt
```

Removing the ipsec configuration from a RADIUS server:

```
switch(config)# no radius-server host 1.1.1.2 vrf mgmt secure ipsec encryption
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.17	The key length for the plaintext value in the key parameter has been increased from 32 to 128 characters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server host tls (RadSec)

```
radius-server host {<FQDN> | <IPV4> | <IPV6>}tls [timeout <TIMEOUT-SECONDS>] [port <PORT-  
NUMBER>][auth-type {pap | chap}] [tracking {enable | disable}] [tracking-  
mode {any | dead-  
only}] [vrf <VRF-NAME>]
```

```
no radius-server host {<FQDN> | <IPV4> | <IPV6>}tls [timeout <TIMEOUT-SECONDS>] [port  
<PORT-  
NUMBER>][auth-type {pap | chap}] [tracking {enable | disable}] [tracking-  
mode {any | dead-  
only}] [vrf <VRF-NAME>]
```

Description

Adds a RadSec server. By default, the RADIUS server is associated with the server group named **radius**. RadSec is used to secure the communication between RADIUS server and RADIUS client using TLS.

The **no** form of this command removes a previously added RadSec server.



The shared key will be added as **radsec** for connection establishment.

Parameter	Description
<code>{<FQDN> <IPv4> <IPv6>}</code>	Specifies the RADIUS server as: ▪ <code><FQDN></code>: a fully qualified domain name. ▪ <code><IPv4></code>: an IPv4 address. ▪ <code><IPv6></code>: an IPv6 address.
<code>tls</code>	Establishes RADIUS connection over TLS.
<code>timeout <TIMEOUT-SECONDS></code>	Specifies the timeout. Range: 1 to 60 seconds. If a timeout is not specified, the value from the global timeout for RADIUS is used.
<code>port <PORT-NUMBER></code>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
<code>auth-type {pap chap}</code>	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the RADIUS global default is used.
<code>acct-port <ACCT-PORT></code>	Specifies the UDP accounting port number. Range: 1 to 65535. Default: 1813.
<code>tracking {enable disable}</code>	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command radius-server tracking to configure RADIUS server tracking globally. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.
<code>tracking-mode {any dead-only}</code>	Configures tracking mode for the RADIUS server that has tracking enabled with the server. The tracking mode is used to monitor the status of RADIUS server reachability. The default tracking mode is any. any Track the RADIUS server irrespective of its server reachability. dead-only Track the RADIUS server only when the server is marked as unreachable.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Examples

Adding a RADIUS server over TLS with an IPv4 address and a named VRF:

```
switch(config)# radius-server host 1.1.1.1 tls vrf mgmt
```

Deleting a RADIUS server over TLS with an IPv4 address and a named VRF:


```
switch(config) # no radius-server host 1.1.1.1 tls vrf mgmt
```

Adding a RADIUS server over TLS with an IPv4 address and default port:

```
switch(config) # radius-server host 1.1.1.1 tls port
```

Deleting a RADIUS server over TLS with an IPv4 address and default port:

```
switch(config) # no radius-server host 1.1.1.1 tls port
```

Adding a RADIUS server over TLS with tracking enabled and tracking mode is set to dead-only:

```
switch(config) # radius-server host 1.1.1.1 tls tracking enable tracking-mode dead-only
```

Deleting a RADIUS server over TLS with tracking enabled and tracking mode is set to dead-only:

```
switch(config) # no radius-server host 1.1.1.1 tls tracking enable tracking-mode dead-only
```

Adding a RADIUS server over TLS with an IPv4 address, a port, and a named VRF:

```
switch(config) # radius-server host 1.1.1.2 tls port 32 vrf mgmt
```

Deleting a RADIUS server over TLS with an IPv4 address, a port, and a named VRF:

```
switch(config) # no radius-server host 1.1.1.2 tls port 32 vrf mgmt
```

Adding a RADIUS server over TLS with an IPv6 address:

```
switch(config) # radius-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334 tls
```

Deleting a RADIUS server over TLS with an IPv6 address:

```
switch(config) # no radius-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334 tls
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

radius-server host tls port-access

```
radius-server host {<FQDN> | <IPV4> | <IPV6>} tls port-access {status-server | keep-alive}
```

```
no radius-server host {<FQDN> | <IPV4> | <IPV6>} tls port-access {status-server | keep-alive}
```

Description

Configures the type of messages to be sent inside RadSec sessions for port access authentication. Default message type for port access authentication sessions is **status-server**.

The **no** form of this command removes the message type configured for port access authentication sessions and sets the default, **status-server**.

Parameter	Description
{<FQDN> <IPV4> <IPV6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPV4>: an IPv4 address. ▪ <IPV6>: an IPv6 address.
port-access {status-server keep-alive}	Specifies the message type to be used for port access authentication in RadSec sessions. Following message types are supported: ▪ status-server: Sets status server message type for authentication. ▪ keep-alive: Sets keep-alive message type for authentication. NOTE: Keep-alive as tracking method and for port access sessions is recommended in networks where a RadSec server is connected to more number of RadSec clients. The server requires additional resources to process status-server and access-request messages when compared to keep-alive messages. This is because status-server and access-request messages are RADIUS protocol packets. However, keep-alive packets are TCP control packets that does not require any additional resources for processing by the RadSec server.

Examples

Configuring the **keep-alive** messages for port access authentication in RadSec session on host **1.1.1.1**:

```
switch(config)# radius-server host 1.1.1.1 tls port-access keep-alive
```

Deleting the message type configured on host **1.1.1.1** for port access authentication session and setting the method to the default, **status-server**:

```
switch(config)# no radius-server host 1.1.1.1 tls port-access status-server
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
9300	config	Administrators or local user group members with execution rights for this command.

radius-server key

```
radius-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]  
no radius-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]
```

Description

Creates or modifies a RADIUS global passkey. The RADIUS global passkey is used as a shared-secret for encrypting the communication between all RADIUS servers and the switch. The RADIUS global passkey is required for authentication unless local passkeys have been set. By default, the RADIUS global passkey is empty. If the administrator has not set this key, the switch will not be able to perform RADIUS authentication. The switch will instead rely on the authentication mechanism configured with **aaa authentication login**.



When this command is entered without parameters, plaintext passkey prompting occurs upon pressing Enter. The entered passkey characters are masked with asterisks.

The **no** form of the command removes the global passkey.

Parameter	Description
plaintext <GLOBAL-PASSKEY>	Specifies the RADIUS global passkey in plaintext format with a length of 1 to 31 characters. As per RFC 2865, a shared-secret can be a mix of alphanumeric and special characters.
ciphertext <GLOBAL-PASSKEY>	Specifies the RADIUS global passkey in encrypted format.

Examples

Adding the global passkey:

```
switch(config)# radius-server key plaintext mypasskey123
```

Adding the global passkey with prompting:

```
switch(config)# radius-server key
Enter the RADIUS server key: *****
Re-Enter the RADIUS server key: *****
```

Removing the global passkey:

```
switch(config)# no radius-server key
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server retries

```
radius-server retries <0-5>
no radius-server retries <0-5>
```

Description

Sets at the global level the number of retries the switch makes before concluding that the RADIUS server is unreachable.

You can override this setting with a fine-grained per RADIUS server retries configuration.

The **no** form of this command resets the RADIUS global retries to the default retries value of 1.

Parameter	Description
retries <0-5>	Specifies the number of retry attempts for contacting RADIUS servers. Range is 0 to 5 retries.

Example

```
switch(config)# radius-server retries 3
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

radius-server service-type in-access-request

```
radius-server service-type in-access-request
no radius-server service-type in-access-request
```

Description

This configuration will include the **Service-Type** RADIUS attribute in Access-Request packets sent to a RADIUS server. The value of the attribute will always be **NAS-Prompt-User**.

The **no** form of this command disables this feature.

Usage

This configuration option is useful for new AOS-CX deployments migrating from a device that is already using this attribute, such as HPE Aruba Networking AOS-S Switches.

Examples

Enabling this switch to send the **Service-Type** RADIUS attribute in Access-Request packets

```
switch(config)# radius-server service-type in-access-request
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.04.1000	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server timeout

```
radius-server timeout [<1-60>]
```

```
no radius-server timeout [<1-60>]
```

Description

Specifies the number of seconds to wait for a response from the RADIUS server before trying the next RADIUS server. If a value is not specified, a default value of 5 seconds is used. You can override this value with a fine-grained per server timeout configured for individual servers.

The **no** form of this command resets the RADIUS global authentication timeout to the default of 5 seconds.

Parameter	Description
timeout <1-60>	Specifies the timeout interval of 1 to 60 seconds. Default: 5 seconds.

Examples

Setting the RADIUS server timeout:

```
switch(config)# radius-server timeout 10
```

Resetting the timeout for the RADIUS server to the default:

```
switch(config)# no radius-server timeout
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

radius-server tls timeout (RadSec)

```
radius-server tls timeout [<1-60>]  
no radius-server tls timeout [<1-60>]
```

Description

Specifies the number of seconds to wait for a response from the RadSec server before trying the next RADIUS or RadSec server. If a value is not specified, a default value of 5 seconds is used. You can override this value with a fine-grained per server timeout configured for individual servers.

The **no** form of this command resets the RadSec global authentication timeout to the default of 5 seconds.

Parameter	Description
timeout <1-60>	Specifies the timeout interval of 1 to 60 seconds. Default: 5 seconds.

Examples

Setting the RadSec server timeout:

```
switch(config)# radius-server tls timeout 10
```

Resetting the timeout for the RadSec to the default:

```
switch(config)# no radius-server tls timeout
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

radius-server tracking

```
radius-server tracking interval <INTERVAL>  
no radius-server tracking interval
```

```
radius-server tracking retries <RETRIES>  
no radius-server tracking retries
```

```
radius-server tracking user-name <NAME>  
    [password [plaintext <PASSWORD> | ciphertext <PASSWORD>]]  
no radius-server tracking user-name <NAME>  
    [password [plaintext <PASSWORD> | ciphertext <PASSWORD>]]
```

Description

Configures RADIUS server tracking settings globally for all configured RADIUS servers that have tracking enabled with the **radius-server host** command on individual servers.

The **no** form of the command removes the specified configuration, reverting it to its default. The no form with **user-name** also clears the password (resets it to empty).

Parameter	Description
<code>interval <INTERVAL></code>	Specifies the time interval, in seconds, to wait before checking the server reachability status. Default: 300. Range 60 to 84600.
<code>retries <RETRIES></code>	Specifies the number of server retries. Default: Global RADIUS retries. Range: 0 to 5.
<code>user-name <NAME></code> <code>[password [plaintext <PASSWORD> </code> <code>ciphertext <PASSWORD>]]</code>	Specifies the user name (and optionally a password) to be used for server checking. The default user name is radius-tracking-user with an empty password. The password is optional and may be entered as plaintext or pasted in as ciphertext. The plaintext password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext. NOTE: When password is entered without a following sub-parameter, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks. NOTE: The user does not have to be configured on the server. Server tracking can still be performed with a user which is not configured on the server because authentication failure on the server achieves confirmation that the server is reachable. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.

Examples

Configuring a tracking interval of 120 seconds:

```
switch(config)# radius-server tracking interval 120
```

Reverting the tracking interval to its default of 300 seconds:

```
switch(config)# no radius-server tracking interval
```

Configuring three retries:

```
switch(config)# radius-server tracking retries 3
```

Configuring user **radius-tracker** with a plaintext password.


```
switch(config)# radius-server tracking user-name radius-tracker
password plaintext track$1
```

Configuring user **radius-tracker** with a prompted plaintext password.

```
switch(config)# radius-server tracking user-name radius-tracker password
Enter the RADIUS server tracking password: *****
Re-Enter the RADIUS server tracking password: *****
```

Reverting the tracking user name to its default of **radius-tracking-user**:

```
switch(config)# no radius-server tracking user-name
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

server

```
server {<FQDN> | <IPV4> | <IPV6>} [tls] [port <PORT-NUMBER>] [vrf <VRF-NAME>]
no server {<FQDN> | <IPV4> | <IPV6>} [tls] [port <PORT-NUMBER>] [vrf <VRF-NAME>]
```

Description

Adds a TACACS+ or RADIUS server to a server group. Only the configured TACACS+ or RADIUS servers are allowed to be added within the server group. If the same server name exists with multiple ports or multiple VRFs, specify the server name, port, and VRF when adding the server to the server-group.

The **no** form of this command removes a TACACS+/RADIUS server from a server-group.

On the HPE Aruba Networking 4100i, 5420, 6000, 6100, 6200, 6300, 6400, 8100, 8325, 8325H, 8325P, 8360, and 10000 Switch series, a RADIUS server can be associated with a maximum of four different user-defined server groups.

On the HPE Aruba Networking 8320, 8400, and 9300/9300S Switch Series, a RADIUS server can be associated with only one user-defined server group.



Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
tls	Specifies the TLS protection for the RADIUS server. If TLS is configured without a port number, the system searches the RADIUS server by host name and sets the default authentication port (2083). Group server priority is assigned based on the sequence in which the servers are added.
port <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default TACACS+ (TCP): 49, RADIUS (UDP): 1812 and RadSec: 2083. If a port number is not provided, the system searches the TACACS+/RADIUS server by host name and sets the default authentication port. Group server priority is assigned based on the sequence in which the servers are added.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Examples

Adding a server to TACACS+ server group sg1 by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server tacacs sg1
switch(config-sg)# server 1.1.1.2 port 32 vrf default
```

Adding a server to TACACS+ server group sg2 by providing an IPv6 address and default VRF:

```
switch(config)# aaa group server tacacs sg2
switch(config-sg)# server 2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf default
```

Adding a server to RADIUS server group sg3 by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server radius sg3
switch(config-sg)# server 1.1.1.5 port 12 vrf default
```

Adding a server to RADIUS server group sg3 with TLS protection by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server radius sg3
switch(config-sg)# server 1.1.1.5 tls port 12 vrf default
```

Adding a server to RADIUS server group sg4 by providing an IPv6 address and default VRF:

```
switch(config)# aaa group server radius sg4
switch(config-sg)# server 2001:0db8:85a3:0000:0000:8a2e:0371:7334 vrf default
```

Adding a server to RADIUS server group sg4 by providing an IPv4 address, port number, and VRF name:

```
switch(config)# aaa group server radius sg4
switch(config-sg)# server 1.1.1.6 port 32 vrf vrf_red
```

Specifying an IPv4 address when removing a TACACS+ server from server group sg1:

```
switch(config)# aaa group server tacacs sg1
switch(config-sg)# no server 1.1.1.2 port 12 vrf default
```

Specifying an IPv6 address when removing a TACACS+ server from server group sg2 with the default VRF:

```
switch(config)# aaa group server tacacs sg2
switch(config-sg)# no server 2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf default
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-sg	Administrators or local user group members with execution rights for this command.

show aaa accounting

show aaa accounting [vsx-peer]

Description

Shows the accounting configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Configuring and then showing the accounting sequence for TACACS+ groups and local:

```
(config)# aaa accounting all-mgmt default start-stop group sgl tacacs radius
(config)# aaa accounting all-mgmt console start-stop local
(config)# aaa accounting all-mgmt ssh start-stop group radius tacacs local
(config)# aaa accounting all-mgmt https-server start-stop group sgl tacacs
(config)# aaa accounting all-mgmt telnet start-stop group radius tacacs local
(config)# show aaa accounting
```

AAA Accounting:

```
Accounting Type           : all
Accounting Mode           : start-stop
Accounting Failthrough    : Enabled
```

Accounting for https-server channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sgl                        | 0
tacacs                    | 1
-----
```

Accounting for console channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----
```

Accounting for default channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
sgl                        | 0
tacacs                    | 1
radius                    | 2
-----
```

Accounting for ssh channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
radius                    | 0
tacacs                    | 1
local                      | 2
-----
```

Accounting for telnet channel:

```
-----
GROUP NAME                | GROUP PRIORITY
-----
radius                    | 0
tacacs                    | 1
local                      | 2
-----
```

Configuring and then showing the accounting sequence for RADIUS groups and local:

```
switch(config)# aaa accounting all default start-stop group rg1 rg2 radius local
switch(config)# aaa accounting all console start-stop group rg4 radius local
switch(config)# exit
switch# show aaa accounting
```

AAA Accounting:

```
Accounting Type           : all
Accounting Mode           : start-stop
Accounting Failthrough    : Enabled
Accounting for default channel:
```

GROUP NAME	GROUP PRIORITY
rg1	0
rg2	1
radius	2
local	3

Accounting for console channel:

GROUP NAME	GROUP PRIORITY
tg4	0
radius	1
local	2

Configuring and then showing only local accounting for default:

```
switch(config)# aaa accounting all default start-stop local
switch(config)# exit
switch# show aaa accounting
AAA Accounting:
Accounting Type           : all
Accounting Mode           : start-stop
Accounting for default channel:
```

GROUP NAME	GROUP PRIORITY
local	0



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authentication

show aaa authentication [vsx-peer]

Description

Shows the authentication configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring TACACS+ authentication sequences and then showing the configuration per connection type (channel):

```
switch(config)# aaa authentication login default group sg1 sg2 sg3 sg4 tacacs local
switch(config)# aaa authentication login ssh group sg1 sg2
switch(config)# aaa authentication login console group sg4 tacacs local
switch(config)# aaa authentication login https-server local group tacacs sg3
switch(config)# aaa authentication login telnet group sg1 sg2
switch(config)# exit
```

```
switch# show aaa authentication
```

```
AAA Authentication:
```

```
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set
```

```
Authentication for ssh channel:
```

GROUP NAME	GROUP PRIORITY
sg1	0
sg2	1

```
Authentication for https-server channel:
```

GROUP NAME	GROUP PRIORITY
local	0
tacacs	1
sg3	2

```
Authentication for console channel:
```

GROUP NAME	GROUP PRIORITY
sg4	0
tacacs	1
local	2

```
Authentication for default channel:
```

GROUP NAME	GROUP PRIORITY
sg1	0
sg2	1
sg3	2
sg4	3

```

tacacs | 4
local | 5
-----
Authentication for telnet channel:
-----
GROUP NAME | GROUP PRIORITY
-----
sg1 | 0
sg2 | 1
-----

```

Configuring RADIUS authentication sequences and then showing the configuration per connection type (channel):

```

switch(config)# aaa authentication login default group rg1 rg2 rg3 rg4 radius local
switch(config)# aaa authentication login console group rg4 radius local
switch(config)# exit
switch# show aaa authentication
AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set

Authentication for default channel:
-----
GROUP NAME | GROUP PRIORITY
-----
rg1 | 0
rg2 | 1
rg3 | 2
rg4 | 3
radius | 4
local | 5
-----

Authentication for console channel:
-----
GROUP NAME | GROUP PRIORITY
-----
rg4 | 0
radius | 1
local | 2
-----

```

Configuring only default authentication and then showing the default connection type (channel):

```

switch(config)# aaa authentication login default local
switch(config)# exit
switch# show aaa authentication

AAA Authentication:
  Fail-through           : Disabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set

Authentication for default channel:

```

GROUP NAME	GROUP PRIORITY
local	0



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa authorization

show aaa authorization [vsx-peer]

Description

Shows the authorization configuration per connection type (channel).

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Configuring and then showing the authorization sequence for default and console connection types (channels):

```
(config)# aaa authorization commands default group sg1 tacacs local
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization commands ssh group sg2
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization commands telnet group sg2
All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization commands console group sg1 local
```



```

All commands will fail if none of the servers in the group list are reachable.
Continue (y/n)? y
(config)# aaa authorization radius ssh group sg1
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y
(config)# aaa authorization radius https-server group sg2
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y

```

```

(config)# show aaa authorization

```

```

***** Command authorization *****

```

```

Authorization for console channel:

```

GROUP NAME	GROUP PRIORITY
sg1	0
local	1

```

Authorization for default channel:

```

GROUP NAME	GROUP PRIORITY
sg1	0
tacacs	1
local	2

```

Authorization for ssh channel:

```

GROUP NAME	GROUP PRIORITY
sg2	0

```

Authorization for telnet channel:

```

GROUP NAME	GROUP PRIORITY
sg2	0

```

***** User authorization through radius *****

```

```

Authorization for ssh channel:

```

GROUP NAME	GROUP PRIORITY
sg1	0

```

Authorization for https-server channel:

```

GROUP NAME	GROUP PRIORITY
sg2	0



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show aaa server-groups

```
show aaa server-groups [tacacs | radius] [vsx-peer]
```

Description

Shows TACACS+ and RADIUS AAA server group information for all server types or for the specified server type.

Parameter	Description
tacacs	Narrows the command output to only TACACS+ servers.
radius	Narrows the command output to only RADIUS servers.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing all AAA server group information:

```
switch# show aaa server-groups

***** AAA Mechanism TACACS+ *****
-----
GROUP NAME      | SERVER NAME                               | PORT | VRF      | PRIORITY
-----
sg2              | 2001:0db8:85a3:0000:0000:8a2e:0370:7334 | 49   | default  | 1
-----
sg1              | 1.1.1.2                                   | 12   | mgmt     | 1
-----
tacacs (default) | FQDN.com                                 | 32   | mgmt     | 1
tacacs (default) | 1.1.1.1                                 | 49   | mgmt     | 2
tacacs (default) | 1.1.1.2                                 | 12   | mgmt     | 3
tacacs (default) | abc.com                                 | 32   | vrf_red  | 4
tacacs (default) | 2001:0db8:85a3:0000:0000:8a2e:0370:7334 | 49   | default  | 5
tacacs (default) | 1.1.1.3                                 | 32   | vrf_blue | 6
```

```

-----
***** AAA Mechanism RADIUS *****
-----
GROUP NAME          | SERVER NAME          | PORT | VRF      | PRIORITY
-----
sg4                  | 2001:0db8:85a3:0000:0000:8a2e:
                    | 0370:7334            | 1812 | default  | 1
-----
sg3                  | 1.1.1.5              | 12   | mgmt     | 1
-----
radius (default)    | 1.1.1.4              | 1812 | mgmt     | 1
radius (default)    | 1.1.1.5              | 12   | mgmt     | 2
radius (default)    | abc1.com              | 32   | mgmt     | 3
radius (default)    | 2001:0db8:85a3:0000:0000:8a2e:
                    | 0370:7334            | 1812 | default  | 4
radius (default)    | 1.1.1.6              | 32   | vrf_red  | 5
radius (default)    | 1.1.1.7              | 32   | vrf_blue | 6
-----

```

Showing TACACS+ server group information:

```

switch# show aaa server-groups tacacs

***** AAA Mechanism TACACS+ *****
-----
GROUP NAME          | SERVER NAME          | PORT | VRF      | PRIORITY
-----
sg2                  | 2001:0db8:85a3:0000:0000:8a2e:
                    | 0370:7334            | 49   | default  | 1
-----
sg1                  | 1.1.1.2              | 12   | mgmt     | 1
-----
tacacs (default)    | FQDN.com              | 32   | mgmt     | 1
tacacs (default)    | 1.1.1.1              | 49   | mgmt     | 2
tacacs (default)    | 1.1.1.2              | 12   | mgmt     | 3
tacacs (default)    | abc.com               | 32   | vrf_red  | 4
tacacs (default)    | 2001:0db8:85a3:0000:0000:8a2e:
                    | 0370:7334            | 49   | default  | 5
tacacs (default)    | 1.1.1.3              | 32   | vrf_blue | 6
-----

```

Showing RADIUS server group information:

```

switch# show aaa server-groups radius

***** AAA Mechanism RADIUS *****
-----
GROUP NAME          | SERVER NAME          | PORT | VRF      | PRIORITY
-----
sg4                  | 2001:0db8:85a3:0000:0000:8a2e:
                    | 0370:7334            | 1812 | default  | 1
-----
sg3                  | 1.1.1.5              | 12   | mgmt     | 1
-----
radius (default)    | 1.1.1.4              | 1812 | mgmt     | 1
radius (default)    | 1.1.1.5              | 12   | mgmt     | 2
radius (default)    | abc1.com              | 32   | mgmt     | 3
radius (default)    | 2001:0db8:85a3:0000:0000:8a2e:
                    | 0370:7334            | 1812 | default  | 4
-----

```

```
radius (default) | 1.1.1.6 | 32 | vrf_red | 5
radius (default) | 1.1.1.7 | 32 | vrf_blue | 6
-----
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show accounting log

```
show accounting log [last <QTY-TO-SHOW> | all]
```

Description

Entered without optional parameters, this command shows all accounting log records for the current boot. Sensitive information is masked from the log, by being represented as asterisks.



This **show accounting log** command replaces the **show audit-log** command that is supported only in 10.00 releases.

Parameter	Description
last <QTY-TO-SHOW>	Specifies how many most-recent accounting log records to show for the current boot. Range: 1 to 1000.
all	Selects for showing, all accounting records from the current boot and the previous boot.

Usage

The log message starts with the record type, which is specific to AOS-CX. Values are the following:

USER_START

Record of a user login action.

USER_END

Record of a user logout action.

USYS_CONFIG

Record of a command executed by the user.

The three types of accounting log information are identified by the **msg=** element starting with the **rec=** item as follows:

- Exec is identified with: **msg='rec=ACCT_EXEC**
- Command is identified with: **msg='rec=ACCT_CMD**
- System is identified with: **msg='rec=ACCT_SYSTEM**

The user group is indicated by **priv-lvl**, which is specific to AOS-CX. Values are the following:

Privilege level	User group
1	operators
15	administrators
19	auditors

The value of **service** indicates which user interface was used:

`service=shell`

Indicates that the log entry is a result of a CLI command.

`service=https-server`

Indicates that the log entry is a result of a REST API request or a Web UI action.

The string value of **data** identifies the CLI command or REST API request that was executed.

These elements are shown in context under *Examples*.

Examples

Showing the accounting log for the previous and current boot. Line breaks have been added for readability.

```
switch# show accounting log all

-----
Local accounting logs from previous boot
-----
----
type=DAEMON_START msg=audit(Nov 05 2018 23:00:58.607:9057) :
auditd start, ver=2.4.3 format=raw kernel=4.9.119-yocto-standard res=success
----
type=USER_START msg=audit(Nov 05 2018 23:06:42.398:42) :
msg='rec=ACCT_EXEC op=start session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:06:42.399:43) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
data="enable" hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:08:24.693:51) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=1
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
data="configure terminal" hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:08:39.108:52) :
```

```

msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=yes
data="https-server rest access-mode read-write"
hostname=8xxx addr=0.0.0.0 res=success'
----
type=USER_START msg=audit(Nov 05 2018 23:10:57.238:58) :
msg='rec=ACCT_EXEC op=start session=REST timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=https-server
data="http-method=POST http-uri=/rest/v1/login"
hostname=8xxx addr=127.0.0.1 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:15:11.958:75) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=yes
data="tacacs-server host 2.2.2.2" hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:15:37.090:76) :
msg='rec=ACCT_CMD op=stop session=REST timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=https-server
data="http-method=GET http-uri=/rest/v1/system/vrfs/mgmt/tacacs_servers"
hostname=8xxx addr=127.0.0.1 res=success'
----
type=USER_END msg=audit(Nov 05 2018 23:26:59.207:90) :
msg='rec=ACCT_EXEC op=stop session=REST timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=https-server
data="http-method=POST http-uri=/rest/v1/logout"
hostname=8xxx addr=127.0.0.1 res=success'
----
type=USER_END msg=audit(Nov 05 2018 23:27:49.164:93) :
msg='rec=ACCT_EXEC op=stop session=CONSOLE timezone=UTC user=user1 priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
hostname=8xxx addr=0.0.0.0 res=success'

-----
Local accounting logs from current boot
-----
----
type=DAEMON_START msg=audit(Nov 05 2018 23:32:05.642:626) :
auditd start, ver=2.4.3 format=raw kernel=4.9.119-yocto-standard res=success
----
type=USER_START msg=audit(Nov 05 2018 23:35:52.915:11) :
msg='rec=ACCT_EXEC op=start session=CONSOLE timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no
hostname=8xxx addr=0.0.0.0 res=success'
----
type=USYS_CONFIG msg=audit(Nov 05 2018 23:35:52.917:12) :
msg='rec=ACCT_CMD op=stop session=CONSOLE timezone=UTC user=admin priv-lvl=15
auth-method=LOCAL auth-type=LOCAL service=shell isconfig=no data="enable"
hostname=8xxx addr=0.0.0.0 res=success'

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#) or Auditor (auditor)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show radius-server

`show radius-server [detail] [vsx-peer]`

Description

Shows configured RADIUS servers information.

Parameter	Description
detail	Selects additional RADIUS server details and global parameters for showing.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

- When the **show radius-server** command shows **None** for the shared-secret, the passkey is missing.
- The **Tracking-Last-Attempted** and **Next-Tracking-Request** fields are applicable only when the RADIUS server tracking method is **access-request**.
- The **TLS Connection Status** section of the output of the **show radius-server detail** command displays the connection status of the TLS connection created for port-access (network client) authentication. If no port-access related configuration is present, the TLS Connection Status field displays a status of **N/A**.

Examples

Showing a summary of the global RADIUS configuration:

```
switch# show radius-server
***** Global RADIUS Configuration *****
```

```
Shared-Secret:<password>
Timeout: 60
Auth-Type: pap
Retries: 5
TLS Timeout: 60
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1
```

```
-----
SERVER NAME                               | TLS | PORT | VRF
-----
20.1.1.129                               |     | 1812 | default
```

1.1.1.4			1812		mgmt
1.1.1.5			12		mgmt
abc1.com			32		mgmt
2001:0db8:85a3:0000:0000:8a2e:0371:7334			1812		default
1.1.1.6			32		vrf_red
1.1.1.7			32		vrf_blue

Showing a summary of a RADIUS server when the status server time interval is configured:

```
switch# show radius-server
Unreachable servers are preceded by *
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds): 400
Number of Servers: 2
-----
SERVER NAME                                | TLS | PORT | VRF
-----
1.1.1.1                                    | Yes | 2083 | default
2.2.2.2                                    |     | 1812 | default
-----
```

Showing details of a global RADIUS configuration:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: ***
Timeout: 5
Auth-Type: pap
Retries: 5
TLS Timeout: 60
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name           : 20.1.1.129
Auth-Port              : 1812
Accounting-Port        : 1813
VRF                    : default
TLS Enabled            : No
Shared-Secret          : None
Timeout                : 60
Retries                : 5
Auth-Type              : pap
Server-Group:Priority   : radius:1
```



```
Tracking                : disabled
Tracking-Mode           : any
Reachability-Status     : N/A
ClearPass-Username      :
ClearPass-Password      : None
```

Showing details of a RADIUS server when the per-server shared key and the global RADIUS shared key are not set:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout : 5
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name           : 1.1.1.1
Auth-Port             : 2083
VRF                   : default
Shared-Secret (default) : None
Timeout (default)     : 5
Retries (default)     : 1
Auth-Type (default)   : pap
Server-Group:Priority  : radius:1
Default-Priority       : 1
```

Showing details of a RADIUS server with TLS:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
TLS Connection Timeout: 5
TLS Connection Retries: 1
Tracking Time Interval (seconds): 60
Tracking Retries: 1
Tracking User-name: jim
Tracking Password: ***
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name           : 172.20.30.30
Auth-Port             : 2083
Accounting-Port       : 2083
VRF                   : default
TLS Enabled           : Yes
TLS Connection Timeout (default): 5
TLS Connection Retries (default): 1
TLS Connection Status : tls_connection_established
Timeout (default)     : 5
Auth-Type (default)   : pap
```

```
Server-Group:Priority      : radius:1
Tracking                  : enabled
Tracking-Mode             : any
Reachability-Status       : reachable
ClearPass-Username        : admin
ClearPass-Password        : ***
```

Showing details of a RADIUS server when the **status-server** tracking method is configured:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds)      : 600
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name                               : 2.2.2.2
Auth-Port                                 : 2083
Accounting-Port                           : 2083
VRF                                        : default
TLS Enabled                               : Yes
TLS Connection Status                     : tls_connection_established
Timeout                                   : 5
Auth-Type                                 : pap
Server-Group:Priority                     : radius:1
Default-Priority                          : 1
ClearPass-Username                        :
ClearPass-Password                        : None
Tracking                                  : disabled
Tracking-Mode                             : any
Tracking-Method                           : status-server
Reachability-Status                       : unknown
Tracking-Last-Attempted                   : N/A
Next-Tracking-Request                     : N/A
Port-Access session                       : status-server
```

Showing details of a RADIUS server when the **keep-alive** tracking method is configured:

```
switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
```

```

Status-Server Time Interval (seconds)      : 400
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name                               : 1.1.1.1
Auth-Port                                  : 2083
Accounting-Port                            : 2083
VRF                                         : default
TLS Enabled                                : Yes
TLS Connection Status                      : tcp_connection_failed
Timeout                                    : 5
Auth-Type                                  : pap
Server-Group:Priority                      : radius:1
ClearPass-Username                        : 
ClearPass-Password                        : None
Tracking                                  : disabled
Tracking-Mode                             : any
Tracking-Method                           : keep-alive
Reachability-Status                       : unknown
Tracking-Last-Attempted                   : N/A
Next-Tracking-Request                     : N/A
Port-Access session                       : status-server

```

Showing details of a RADIUS server when the **access-request** tracking method is configured:

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 300
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Status-Server Time Interval (seconds)      : 500
Number of Servers: 1

***** RADIUS Server Information *****
Server-Name                               : 4.4.4.4
Auth-Port                                  : 2083
Accounting-Port                            : 2083
VRF                                         : default
TLS Enabled                                : Yes
TLS Connection Status                      : tcp_connection_failed
Timeout                                    : 5
Auth-Type                                  : pap
Server-Group:Priority                      : radius:1
ClearPass-Username                        : 
ClearPass-Password                        : None
Tracking                                  : disabled
Tracking-Mode                             : any
Tracking-Method                           : access-request
Reachability-Status                       : unknown
Tracking-Last-Attempted                   : N/A
Next-Tracking-Request                     : N/A
Port-Access session                       : keep-alive

```

Showing details of a RADIUS server when the server group is configured:

```

switch# show radius-server detail
***** Global RADIUS Configuration *****

Shared-Secret: None
Timeout: 10
Auth-Type: pap
Retries: 5
TLS Timeout: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius
Tracking Password: None
Status-Server Time Interval (seconds): 300
Number of Servers: 12
AAA Server Status Trap: Enabled

***** RADIUS Server Information *****
Server-Name           : cppm2.cxsecurity.com
Auth-Port             : 1812
Accounting-Port       : 1813
VRF                   : sss
TLS Enabled           : No
Shared-Secret         : ***
Timeout               : 10
Retries               : 5
Auth-Type             : pap
Server-Group:Priority : RG1:1, RG2:1, RG3:1, RG4:1
ClearPass-Username    :
ClearPass-Password    : None
Tracking              : enabled
Tracking-Mode         : any
Reachability-Status   : reachable, Since Tue Mar 14 19:58:45 UTC 2023
Tracking-Last-Attempted : Thu Mar 16 10:23:46 UTC 2023
Next-Tracking-Request : 36 seconds

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius-server secure ipsec

```

show radius-server secure ipsec { server-list | host {<FQDN> | <IPv4> | <IPv6>}
[port <PORT-NUMBER>] [vrf <VRF-NAME>] [vsx-peer] }

```

Description

Shows information for one or all RADIUS servers configured with IPsec.

Parameter	Description
<code>server-list</code>	Selects all servers for showing.
<code>{<FQDN> <IPv4> <IPv6>}</code>	Specifies the RADIUS server as: ▪ <code><FQDN></code>: a fully qualified domain name. ▪ <code><IPv4></code>: an IPv4 address. ▪ <code><IPv6></code>: an IPv6 address.
<code>port <PORT-NUMBER></code>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
<code>vrf <VRF-NAME></code>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

The IPsec key is shown in an exportable ciphertext format.

Examples

Showing information for RADIUS server 1.1.1.1 secured with IPsec:

```
switch# show radius-server secure ipsec host 1.1.1.1
IPsec                : enabled
Protocol              : ESP
Authentication        : MD5
Encryption            : AES
SPI                   : 1234
```

Showing information for all RADIUS servers secured with IPsec:

```
switch# show radius-server secure ipsec server-list
Server                : 1.1.1.1
IPsec                 : enabled
Protocol              : ESP
Authentication        : MD5
Encryption            : AES
SPI                   : 1234

Server                : 1.1.1.2
IPsec                 : enabled
Protocol              : ESP
Authentication        : MD5
Encryption            : AES
SPI                   : 12341
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius-server authentication statistics

show radius-server statistics authentication [vsx-peer]

Description

Shows authentication statistics for all configured RADIUS servers.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing RADIUS server authentication statistics:

```
switch# show radius-server statistics authentication
Server Name      : rad1
Auth-Port        : 1812
Accounting-Port  : 1813
VRF              : mgmt
TLS Enabled      : Yes

Authentication Statistics
-----
Round Trip Time   : 100
Pending Requests  : 0
Timeouts          : 6
Bad Authenticators : 2
Packets Dropped   : 0
Access Requests   : 20
Access Challenge   : 8
Access Accepts     : 14
Access Rejects     : 0
Access Response Malformed : 0
Access Retransmits : 0
Tracking Requests : 5
```

```
Tracking Responses      : 5
Unknown Response Code   : 0
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show radius-server authentication statistics host

```
show radius-server statistics authentication host {<FQDN> | <IPv4> | <IPv6>}
[tls] [port <PORT-NUMBER>] [vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows authentication statistics for the specified RADIUS server.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the RADIUS server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
<i>tls</i>	Selects TLS.
<i>port</i> <PORT-NUMBER>	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
<i>vrf</i> <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.
<i>vsx-peer</i>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing RADIUS server authentication statistics:

```

switch# show radius-server statistics authentication host 20.1.1.49
Server Name       : 20.1.1.49
Auth-Port        : 2083
Accounting-Port   : 2083
VRF              : default
TLS Enabled      : No

Authentication Statistics
-----
Round Trip Time   : 3
Pending Requests  : 0
Timeouts         : 0
Bad Authenticators : 0
Packets Dropped   : 0
Access Requests   : 13
Access challenge   : 6
Access Accepts    : 3
Access Rejects    : 4
Access Response Malformed : 0

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tacacs-server

show tacacs-server [detail] [vsx-peer]

Description

Shows the configured TACACS+ servers.

Parameter	Description
detail	Selects additional TACACS+ server details and global parameters for showing.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing a summary of a global TACACS+ configuration with a shared-secret:

```
switch# show tacacs-server
***** Global TACACS+ Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8elcA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Number of Servers: 5

-----
SERVER NAME                               | PORT | VRF
-----
1.1.1.1                                  | 49   | mgmt
1.1.1.2                                  | 12   | mgmt
abc.com                                  | 32   | vrf_blue
2001:0db8:85a3:0000:0000:8a2e:0370:7334 | 49   | default
1.1.1.3                                  | 32   | vrf_red
-----
```

Showing details of a global TACACS+ configuration:

```
switch# show tacacs-server detail
***** Global TACACS+ Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8elcA+CyD0RvfbeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Number of Servers: 5

***** TACACS+ Server Information *****

Server-Name      : 1.1.1.2
Auth-Port        : 12
VRF              : mgmt
Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout (default)  : 5
Auth-Type (default) : pap
Server-Group      : sg1
Group-Priority    : 1

Server-Name      : 2001:0db8:85a3:0000:0000:8a2e:0370:7334
Auth-Port        : 49
VRF              : default
Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout (default)  : 5
Auth-Type (default) : pap
Server-Group      : sg2
Group-Priority    : 1

Server-Name      : 1.1.1.1
Auth-Port        : 49
VRF              : mgmt
Shared-Secret (default) : AQBapb+HsdpqVlQ3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout (default)  : 5
Auth-Type (default) : pap
Server-Group (default) : tacacs
Default-Priority   : 1

Server-Name      : abc.com
Auth-Port        : 32
VRF              : vrf_red
```

```

Shared-Secret (default) : AQBapb+HsdpqV1Q3CPCBMQTG8eeA8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout                  : 15
Auth-Type (default)     : pap
Server-Group (default)  : tacacs
Default-Priority         : 3

Server-Name              : 1.1.1.3
Auth-Port                : 32
VRF                      : vrf_blue
Shared-Secret            : AQBapfnqbSSwqKC476tdUFZ+AncIRY92hDTYkQCAAAAFEaHn43vNC
Timeout                  : 15
Auth-Type                : chap
Server-Group (default)  : tacacs
Default-Priority         : 5

```

Showing TACACS+ server when per-server shared key and global TACACS+ shared key is not set:

```

switch# show tacacs-server
***** Global TACACS+ Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Number of Servers: 1

-----
SERVER NAME                               | PORT | VRF
-----
1.1.1.1                                  | 49   | default
-----

```

Showing TACACS+ server details when per-server shared key and global TACACS+ shared key is not set:

```

switch# show tacacs-server detail
***** Global TACACS+ Configuration *****

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Number of Servers: 1

***** TACACS+ Server Information *****
Server-Name          : 1.1.1.1
Auth-Port            : 49
VRF                  : default
Shared-Secret (default) : None
Timeout (default)    : 5
Auth-Type (default)  : pap
Server-Group (default) : tacacs
Default-Priority      : 1

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tacacs-server statistics

show tacacs-server statistics [vsx-peer]

Description

Shows authentication statistics for all configured TACACS+ servers.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing TACACS+ server authentication statistics:

```
switch# show tacacs-server statistics
Server Name      : tac1
Auth-Port       : 49
VRF             : mgmt
Authentication Statistics
-----
Round Trip Time      : 1
Pending Requests    : 0
Timeout            : 0
Unknown Types       : 0
Packet Dropped      : 0
Auth Start          : 8
Auth challenge       : 0
Auth Accepts        : 4
Auth Rejects        : 4
Auth reply malformed : 0
Tracking Requests    : 0
Tracking Responses   : 0
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show tech aaa

show tech aaa

Description

Shows the AAA configuration settings.

Example

Showing the AAA configuration settings:

```
switch# show tech aaa

=====
Show Tech executed on Tue Feb 14 02:19:11 2017
=====
[Begin] Feature aaa
=====

*****
Command : show aaa authentication
*****
AAA Authentication:
  Fail-through           : Enabled
  Limit Login Attempts   : Not set
  Lockout Time           : 300
  Minimum Password Length : Not set

Authentication for ssh channel:

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

Authentication for https-server channel:

-----
GROUP NAME                | GROUP PRIORITY
-----
local                      | 0
-----

Authentication for console channel:
-----
```

```
GROUP NAME | GROUP PRIORITY
```

```
-----  
local | 0  
-----
```

Authentication for default channel:

```
-----  
GROUP NAME | GROUP PRIORITY
```

```
-----  
tacacs | 0  
local | 1  
-----
```

Authentication for telnet channel:

```
-----  
GROUP NAME | GROUP PRIORITY
```

```
-----  
local | 0  
-----
```

```
*****
```

```
Command : show aaa accounting
```

```
*****
```

```
AAA Accounting:
```

```
Accounting for default channel:
```

```
Accounting Type : all
```

```
Accounting Mode : start-stop
```

```
Default Accounting for login Channels:
```

```
-----  
GROUP NAME | GROUP PRIORITY
```

```
-----  
local | 0  
-----
```

Accounting for ssh channel:

```
-----  
GROUP NAME | GROUP PRIORITY
```

```
-----  
tacacs | 0  
local | 1  
-----
```

Accounting for https-server channel:

```
-----  
GROUP NAME | GROUP PRIORITY
```

```
-----  
tacacs | 0  
-----
```

Accounting for telnet channel:

```
-----  
GROUP NAME | GROUP PRIORITY
```

```
-----  
tacacs | 0  
local | 1  
-----
```

```
*****
```

```
Command : show aaa accounting port-access
```

```
*****
```

```

...
AAA Accounting Port Access
=====
Radius Accounting Enabled      : yes
Radius Server Group           : acct_group
Local Accounting Enabled       : no
Accounting Mode                : start-stop
Interim Update Enabled         : true
Interim Interval               : 12 minutes
Interim Update on-reauth Enabled : true
...

*****
Syntax  : show aaa accounting port-access interface <IFNAME | all> client-status
[mac <MAC-ADDRESS>]
Command : show aaa accounting port-access interface 1/1/1 client-status
*****
...

Port Access Client Status Details

Client 00:50:56:96:5b:9f, steve
=====
Session Details
-----
Port           : 1/1/22
Session Time    : 141s
IPv4 Address    : 10.0.0.3
IPv6 Address    : 2001::1
                2001::3

Accounting Details
-----
Accounting Session ID : 1584556574841
Input Packets         : 265
Input Octets          : 28348
Output Packets        : 341
Output Octets         : 37761
Input Gigaword        : 0
Output Gigaword       : 0
...

...

#### No aaa clients

When there are no port-access accounting sessions:

...

switch# show aaa accounting port-access interface all client-status
Port-access accounting sessions not found.

switch# show aaa accounting port-access interface 1/1/2 client-status
Port-access accounting sessions not found.

switch# show aaa accounting port-access interface 1/1/2 client-status mac
6e:93:79:d9:cb:ee
Port-access accounting sessions not found.
...

*****
Syntax  : show accounting log {all | port-access}

```

```

Command : show accounting log port-access
*****
Command to display the Local accounting logs for the network user.
...
-----
May 29 2018 20:29:03.714:53 'acct-id=56789453 type=network user=NWUSER auth-
method=dot1x auth-type=radius rec=ACCT_START mac=00:0d:6a:4f:2a:44 input-pkt=0
ouput-pkt=0 input-octet=0 output-octets=0'
-----
May 29 2018 20:30:03.714:53 'acct-id=56789453 type=network user=NWUSER auth-
method=dot1x auth-type=radius rec=ACCT_INTRM mac=00:0d:6a:4f:2a:44 input-pkt=2
ouput-pkt=30 input-octet=20 output-octets=50'
-----
May 29 2018 24:29:03.714:53 'acct-id=56789453 type=network user=NWUSER auth-
method=dot1x auth-type=radius rec=ACCT_STOP mac=00:0d:6a:4f:2a:44 input-pkt=20
ouput-pkt=300 input-octet=200 output-octets=500'
-----
May 29 2018 20:29:03.714:53 'acct-id=56789453 type=network user=NWUSER aauth-
method=macauth auth-type=local rec=ACCT_START mac=00:0d:6a:4f:2a:44 input-pkt=0
ouput-pkt=0 input-octet=0 output-octets=0'
-----
...

*****
Syntax : show radius-server statistics {authentication | accounting}
*****
*****
Command : show radius-server statistics authentication
*****
...

Server Name      : 2.2.2.2
Auth-Port       : 1812
Accounting-Port : 1813
VRF             : mgmt

Authentication Statistics
-----
Round Trip Time      : 100
Pending Requests    : 0
Timeouts            : 6
Bad Authenticators   : 2
Packets Dropped     : 0
Access Requests     : 20
Access Challenge    : 8
Access Accepts      : 14
Access Rejects      : 0
Access Response Malformed : 0
Access Retransmits  : 0
Tracking Requests   : 5
Tracking Responses  : 5
Unknown Response Code : 0
...

*****
Command : show radius-server statistics accounting
*****
...

Server Name      : 2.2.2.2
Auth-Port       : 1812
Accounting-Port : 1813
VRF             : mgmt

Accounting Statistics

```

```

-----
Round Trip Time           : 100
Pending Requests         : 0
Timeouts                 : 5
Bad Authenticators       : 1
Packets Dropped          : 0
Accounting Requests      : 15
Accounting Responses     : 10
Accounting Response Malformed : 0
Accounting Retransmits   : 0
Unknown Response Code    : 0
...

*****
Command : show aaa authorization
*****

Authorization for default channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
local                     | 0
-----

Authorization for console channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
local                     | 0
-----

Authorization for ssh channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
tacacs                   | 0
local                    | 1
-----

Authorization for telnet channel:
-----
GROUP NAME                | GROUP PRIORITY
-----
tacacs                   | 0
local                    | 1
-----

*****
Command : show aaa server-groups
*****

***** AAA Mechanism TACACS+ *****
-----
-----
GROUP NAME                | SERVER NAME                | PORT | PRIORITY | VRF
-----
tacacs                   | 1.1.1.1                   | 49   | 1        |
mgmt
-----
-----

```



```

***** AAA Mechanism RADIUS *****
-----
GROUP NAME | SERVER NAME | PORT | PRIORITY | VRF
-----

*****
Command : show tacacs-server detail
*****
***** Global TACACS+ Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8ekK1c...fba8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Tracking Time Interval (seconds): 300
Tracking User-name: tacacs-tracking-user
Tracking Password: None
Number of Servers: 1

***** TACACS+ Server Information *****
Server-Name : 1.1.1.1
Auth-Port : 49
VRF : mgmt
Shared-Secret : AQBapfiTREwB7yUKCdmOMT0f...9j2AUxlGAAAAF2MkfMTtojQX

Timeout : 5
Auth-Type : pap
Server-Group : tacacs
Default-Priority : 1
Tracking : disabled
Reachability-Status : N/A

*****
Command : show radius-server detail
*****
***** Global RADIUS Configuration *****

Shared-Secret: AQBapb+HsdpqVlQ3CPCBMQTG8ekK1cA+Cy...8BEgikCgAAAJOWZSNzA2SWrLA=
Timeout: 5
Auth-Type: pap
Retries: 1
Number of Servers: 0

=====
[End] Feature aaa
=====

=====
Show Tech commands executed successfully
=====

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

tacacs-server auth-type

```
tacacs-server auth-type {pap | chap}
no tacacs-server auth-type [pap | chap]
```

Description

Enables the CHAP or PAP authentication protocol, which is used for communication with the TACACS+ servers, at the global level. You can override this command with a fine-grained per server **auth-type** configuration.

The **no** form of this command resets the global authentication mechanism for TACACS+ to PAP, which is the default authentication mechanism for TACACS+.

Parameter	Description
auth-type {pap chap}	Selects either the PAP or CHAP authentication protocol.

Examples

Enabling command for CHAP authentication:

```
switch(config)# tacacs-server auth-type chap
```

Enabling command for PAP authentication:

```
switch(config)# tacacs-server auth-type pap
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server host

```
tacacs-server host {<FQDN> | <IPv4> | <IPv6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [tracking {enable | disable}] [vrf <VRF-NAME>]
```

```
no tacacs-server host {<FQDN> | <IPv4> | <IPv6>}  
    [key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]  
    [timeout <TIMEOUT-SECONDS>] [port <PORT-NUMBER>]  
    [auth-type {pap | chap}] [tracking {enable | disable}] [vrf <VRF-NAME>]
```

Description

Adds a TACACS+ server. By default, the TACACS+ server is associated with the server group named **tacacs**.

The **no** form of this command removes a previously added TACACS+ server.

Parameter	Description
{<FQDN> <IPv4> <IPv6>}	Specifies the TACACS+ server as: ▪ <FQDN>: a fully qualified domain name. ▪ <IPv4>: an IPv4 address. ▪ <IPv6>: an IPv6 address.
key [plaintext <PASSKEY> ciphertext <PASSKEY>]	Selects either a plaintext or an encrypted local shared-secret passkey for the server. As per RFC 2865, shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 128 alphanumeric and special characters. NOTE: When key is entered without either sub-parameter, plaintext passkey prompting occurs upon pressing Enter. Enter must be pressed immediately after the key parameter without entering other parameters. The entered passkey characters are masked with asterisks. When key is omitted, the server uses the global passkey. This command requires either the global or local passkey to be set; otherwise the server will not be contacted. Command tacacs-server key is available for setting the global passkey.
timeout <TIMEOUT-SECONDS>	Specifies the timeout. Range: 1 to 60 seconds. Default : 5 seconds.
port <PORT-NUMBER>	Specifies the TCP authentication port number. Range: 1 to 65535. Default: 49.
auth-type {pap chap}	Selects either the PAP (the default) or CHAP authentication types. If this parameter is not specified, the TACACS+ global default is used.
tracking {enable disable}	Enables or disables server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable. Use command tacacs-server tracking to configure TACACS+ server tracking globally.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used.

Usage

If the fully qualified domain name is provided for the TACACS+ server, a DNS server must be configured and accessible through the same VRF which is configured for the TACACS+ server. This configuration is required for the resolution of the TACACS+ server hostname to its IP address. If a DNS server is not available for this VRF, the TACACS+ servers reachable through this VRF must be configured by means of their IP addresses only.

Examples

Adding a TACACS+ server with an IPv4 address, plaintext passkey, timeout, port, authentication type, and VRF name:

```
switch(config)# tacacs-server host 1.1.1.3 key plaintext test-123 timeout 15 port 32 auth-type chap vrf vrf_red
```

Adding a TACACS+ server with an IPv4 address and prompted plaintext passkey:

```
switch(config)# tacacs-server host 1.1.1.5 key  
Enter the TACACS server key: *****  
Re-Enter the TACACS server key: *****
```

Adding a TACACS+ server with an IPv4 address and a named VRF:

```
switch(config)# tacacs-server host 1.1.1.1 vrf mgmt
```

Adding a TACACS+ server with an IPv4 address, a port, and a named VRF:

```
switch(config)# tacacs-server host 1.1.1.2 port 32 vrf mgmt
```

Adding a TACACS+ server with an FQDN, a timeout, port number, and a named VRF:

```
switch(config)# tacacs-server host abc.com timeout 15 port 32 vrf vrf_blue
```

Adding a TACACS+ server with an IPv6 address:

```
switch(config)# tacacs-server host 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Deleting a TACACS+ server with an IPv4 address and specified VRF:

```
switch(config)# no tacacs-server host 1.1.1.1 vrf mgmt
```

Deleting a TACACS+ server with an FQDN, port, and specified VRF:

```
switch(config)# no tacacs-server host abc.com port 32 vrf vrf_blue
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.17	The key length for the plaintext value in the key parameter has been increased from 32 to 128 characters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server key

```
tacacs-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]  
no tacacs-server key [plaintext <GLOBAL-PASSKEY> | ciphertext <GLOBAL-PASSKEY>]
```

Description

Creates or modifies a TACACS+ global passkey. The TACACS+ global passkey is used as a shared-secret for encrypting the communication between all TACACS+ servers and the switch. The TACACS+ global passkey is required for authentication unless local passkeys have been set. By default, the TACACS+ global passkey is empty. If the administrator has not set this key, the switch will not be able to perform TACACS+ authentication. The switch will instead rely on the authentication mechanism configured with **aaa authentication login**.



When this command is entered without parameters, plaintext passkey prompting occurs upon pressing Enter. The entered passkey characters are masked with asterisks.

The **no** form of the command removes the global passkey.

Parameter	Description
plaintext <GLOBAL-PASSKEY>	Specifies the TACACS+ global passkey in plaintext format with a length of 1 to 128 characters. As per RFC 2865, a shared-secret can be a mix of alphanumeric and special characters.
ciphertext <GLOBAL-PASSKEY>	Specifies the TACACS+ global passkey in encrypted format.

Examples

Adding the global passkey:

```
switch(config)# tacacs-server key plaintext mypasskey123
```

Adding the global passkey with prompting:

```
switch(config)# tacacs-server key
```

```
Enter the TACACS server key: *****
Re-Enter the TACACS server key: *****
```

Removing the global passkey:

```
switch(config)# no tacacs-server key
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.17	The key length for the plaintext parameter is increased from 32 to 128 characters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server timeout

```
tacacs-server timeout [<1-60>]
no tacacs-server timeout [<1-60>]
```

Description

Specifies the number of seconds to wait for a response from the TACACS+ server before trying the next TACACS+ server. If a value is not specified, a default value of 5 seconds is used. You can override this value with a fine-grained per server timeout configured for individual servers.

The **no** form of this command resets the TACACS+ global authentication timeout to the default of 5 seconds.

Parameter	Description
timeout <1-60>	Specifies the timeout interval of 1 to 60 seconds. Default: 5 seconds.

Examples

Specifying the TACACS+ server timeout:

```
switch(config)# tacacs-server timeout 10
```

Resetting the timeout for the TACACS+ server to the default:

```
switch(config)# no tacacs-server timeout
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

tacacs-server tracking

```
tacacs-server tracking interval <INTERVAL>
no tacacs-server tracking interval [<INTERVAL>]
```

```
tacacs-server tracking user-name <NAME>
    [password [plaintext <PASSWORD> | ciphertext <PASSWORD>]]
no tacacs-server tracking [user-name [<NAME>] [ciphertext <PASSWORD>]]
```

Description

Configures TACACS+ server tracking settings globally for all configured TACACS+ servers that have tracking enabled with the **tacacs-server host** command on individual servers.

The **no** form of the command removes the specified configuration, reverting it to its default. The no form with **user-name** also clears the password (resets it to empty).

Parameter	Description
<code>interval <INTERVAL></code>	Specifies the time interval, in seconds, to wait before checking the server reachability status. Default: 300. Range 60 to 84600.
<code>user-name <NAME></code> <code>[password [plaintext <PASSWORD> </code> <code>ciphertext <PASSWORD>]]</code>	Specifies the user name (and optionally a password) to be used for server checking. The default user name is tacacs-tracking-user with an empty password. The password is optional and may be entered as plaintext or pasted in as ciphertext. The plaintext password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext. NOTE: When password is entered without a following sub-parameter, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Parameter	Description
	NOTE: The user does not have to be configured on the server. Server tracking can still be performed with a user which is not configured on the server because authentication failure on the server achieves confirmation that the server is reachable. NOTE: Server tracking uses authentication request and response packets to determine server reachability status. The server tracking user name and password are used to form the request packet which is sent to the server with tracking enabled. Upon receiving a response to the request packet, the server is considered to be reachable.

Examples

Configuring a tracking interval of 120 seconds:

```
switch(config)# tacacs-server tracking interval 120
```

Reverting the tracking interval to its default of 300 seconds:

```
switch(config)# no tacacs-server tracking interval
```

Configuring user **tacacs-tracker** with a plaintext password.

```
switch(config)# tacacs-server tracking user-name tacacs-tracker password plaintext track$1
```

Configuring user **tacacs-tracker** with a prompted plaintext password.

```
switch(config)# tacacs-server tracking user-name tacacs-tracker password
Enter the TACACS server tracking password: *****
Re-Enter the TACACS server tracking password: *****
```

Reverting the tracking user name to its default of **tacacs-tracking-user**:

```
switch(config)# no tacacs-server tracking user-name
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

clear accounting-logs

clear accounting-logs

Description

Use this command to clear accounting logs. Once issued, only logs generated after this command is run will be displayed in the output of the **show accounting log** commands.



This command will not clear logs when the [logging accounting-format-native](#) feature is configured. To clear accounting logs on switches with this feature enabled, users should first revert the native accounting format back to the default AOS-CX format by executing the **no logging accounting-format-native** command.

Example

```
switch(config)# clear accounting-logs
```

The following example shows that accounting logs cannot be cleared using the clear accounting-logs command if the **logging accounting-native-format** command has been enabled, and that disabling this option with the **no logging accounting-format-native** command again allows the accounting logs to be cleared.

```
switch# logging audit-format-native
switch# clear accounting-logs
Warning: Clear accounting-logs is not supported for 'audit-format-native'.
switch# no logging audit-format-native
switch# clear accounting-logs
switch# show accounting log last 5
-----
Command logs from current boot
-----
No command logs has been logged in the system
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

diag persistent-storage

```
diag persistent-storage enable [{severity <LEVEL> | timeout <TIMEOUT> | filter <FILTER_NAME> | storage-writes <STORAGE_WRITES> | usb <STORAGE_URL>}]
diag persistent-storage disable
```

Description

Enables or disables storage of logs in storage. Only logs of the specified severity and above will be preserved in the storage.



To switch the persistent storage setting from one option (e.g., USB) to another (e.g., storage-writes), you must first disable persistent storage by running the command `diag persistent-storage disable`. Note that the storage-writes option applies only to local storage and does not work with USB.

Parameter	Description
<code>enable</code>	Enable persistent logging.
<code>disable</code>	Disable persistent logging.
<code>severity <LEVEL></code>	Specifies the severity of the syslog messages: ▪ alert: Preserves syslog messages with the severity of alert (6) and emergency (7) ▪ crit: Preserves syslog messages with the severity of critical (5) and above. Default. ▪ debug: Preserves syslog messages with the severity of debug (0) and above. ▪ emer: Preserves syslog messages with the severity of emergency (7) only. ▪ err: Preserves syslog messages with the severity of err (4) and above. ▪ info: Preserves syslog messages with the severity of info (1) and above. ▪ notice: Preserves syslog messages with the severity of notice (2) and above. ▪ warn: Preserves syslog messages with the severity of warning (3) and above.
<code>filter <FILTER_NAME></code>	Preserve logs for specified filter name.
<code>timeout <TIMEOUT></code>	Preserve logs for specified duration. Range: 1 to 60 minutes. Default: 20 minutes.
<code>storage-writes <STORAGE_WRITES></code>	Limit the amount of storage writes.
<code>usb <STORAGE_URL></code>	Preserve logs in the USB storage.

Examples

Enabling storage of logs in storage with severity **err** and timeout 30 minutes:

```
switch(config)#diag persistent-storage enable severity err timeout 30
Logs will be written to storage. Prolonged usage of persistent logging can affect
lifetime of storage. Hence enable persistent logging only for short duration and
also for the right severity.
Do you want to continue (y/n)? y
```

Enabling storage of logs in storage with severity **err** and **timeout** 30 minutes and 512 storage-writes:

```
switch(config)#diag persistent-storage enable severity err timeout 30 storage-
writes 512
Logs will be written to storage. Prolonged usage of persistent logging can affect
lifetime of storage. Hence enable persistent logging only for short duration and
also for the right severity.
Do you want to continue (y/n)? y
```

Disabling log storage:

```
switch(config)# diag persistent-storage disable
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

logging

```
logging {<IPV4-ADDR> | <IPV6-ADDR> | <FQDN | HOSTNAME>} {udp [<PORT-NUM>]}|{tcp [<PORT-
NUM>]}|{tls [<PORT-NUM>]}
  auth-mode {certificate|subject-name}
  disable
  filter <FILTER-NAME>
  include-auditable-events
  legacy-tls-renegotiation]
  rate-limit-burst <BURST>
  rate-limit-interval <INTERVAL>] ]
  severity <LEVEL>]
  vrf <VRF-NAME>]
```

no logging { <IPV4-ADDR> | <IPV6-ADDR> | <FQDN | HOSTNAME> }

Description

Enables syslog forwarding to a remote syslog server.

The **no** form of this command disables syslog forwarding to a remote syslog server.

Starting with AOS-CX 10.11, payload information is present in accounting logs.

The maximum REST payload that can be sent to RADIUS/TACACS server is 1024 characters, and the maximum of REST payload that can be sent to syslog server is 3500 characters. If this limit is reached, the log will display three dots (...) to indicate that the log exceeded the character limit and is incomplete.

Parameter	Description
{ <IPV4-ADDR> <IPV6-ADDR> <HOSTNAME> }	Selects the IPv4 address, IPv6 address, or host name of the remote syslog server. Required.
[udp [<PORT-NUM>] tcp [<PORT-NUM> tls [<PORT-NUM>]]	Specifies the UDP port, TCP port, or TLS port of the remote syslog server to receive the forwarded syslog messages.
udp [<PORT-NUM>]	Range: 1 to 65535. Default: 514
tcp [<PORT-NUM>]	Range: 1 to 65535. Default: 1470
tls [<PORT-NUM>]	Range: 1 to 65535. Default: 6514
auth-mode	Specifies the TLS authentication mode used to validate the certificate. ▪ certificate: Validates the peer using trust anchor certificate based authentication. Default. ▪ subject-name: Validates the peer using trust anchor certificates as well as subject-name based authentication.
disable	Disable remote syslog configuration. This does not delete the configuration, just disables/pauses the forwarding of syslog messages to the remote server. The config/forwarding can be reenabled (un-paused) again using the no logging <hostname> disable command.
filter <FILTER-NAME>	Specifies the name of the filter to be applied on the syslog messages.
include-auditable-events	Specifies that auditable messages are also logged to the remote syslog server.
legacy-tls-renegotiation	Enables the TLS connection with a remote syslog server supporting legacy renegotiation.
rate-limit-burst <BURST>	Specifies the rate limit for the messages sent to the remote syslog server.
rate-limit-interval <INTERVAL>	Specifies the rate limit interval in seconds. Default: 30

Parameter	Description
	Seconds
<code>severity <LEVEL></code>	Specifies the severity of the syslog messages: ▪ alert: Forwards syslog messages with the severity of alert (6) and emergency (7). ▪ crit: Forwards syslog messages with the severity of critical (5) and above. ▪ debug: Forwards syslog messages with the severity of debug (0) and above. ▪ emerg: Forwards syslog messages with the severity of emergency (7) only. ▪ err: Forwards syslog messages with the severity of err (4) and above ▪ info: Forwards syslog messages with the severity of info (1) and above. Default. ▪ notice: Forwards syslog messages with the severity of notice (2) and above. ▪ warning: Forwards syslog messages with the severity of warning (3) and above.
<code>vrf <VRF-NAME></code>	Specifies the VRF used to connect to the syslog server. Optional. Default: <code>default</code>

Examples

Enabling the syslog forwarding to remote syslog server 10.0.10.2:

```
switch(config)# logging 10.0.10.2
```

Enabling the syslog forwarding of messages with a severity of **err (4)** and above to TCP port 4242 on remote syslog server 10.0.10.9 with VRF **lab_vrf**:

```
switch(config)# logging 10.0.10.9 tcp 4242 severity err vrf lab_vrf
```

Disabling syslog forwarding to a remote syslog server:

```
switch(config)# no logging
```

Enabling syslog forwarding over TLS to a remote syslog server using subject-name authentication mode:

```
switch(config)# logging example.com tls auth-mode subject-name
```

Applying log filtering for syslog server forwarding:

```
switch(config)# logging 10.0.10.6 severity info filter filter_lldp_logs vrf mgmt
```

Applying log filtering and enabling the rate limit for syslog server forwarding over TCP port:

```
switch(config)# logging 10.0.10.2 tcp 3440 severity err vrf mgmt include-  
auditable-events filter filter_lldp_logs rate-limit-burst 3 rate-limit-interval 35
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.12.1000	The disable parameter is introduced
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

logging accounting-format-native

```
logging accounting-format-native  
[no] logging accounting-format-native
```

Description

Change the accounting log message format to native Linux format. (Default: AOS-CX format)
The 'no' form of this command will change the accounting log message format to AOS-CX format.

Usage

This option enables the switch to show all types of accounting records to the user. When configured, the same format will be used while sending messages to syslog servers. When upgrading to this version of AOS-CX from AOS-CX 10.10 or earlier versions, if native accounting logs are preferred, then best practices is to issue this command as a part of the upgrade. If the switch upgrades from AOS-CX 10.10 or earlier without configuring this setting, by default, the accounting log message format will be AOS-CX Format.

Example

This example changes the accounting log message format to native Linux format.

```
switch(config)# logging accounting-format-native
```

The following example returns the accounting log message format to the default AOS-CX format.

```
switch(config)# no logging accounting-format-native
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

logging filter

```
logging filter <FILTER-NAME>
```

```
[{enable | disable}]
```

```
[<SEQUENCE-ID>] {permit | deny} [event-id <EVENT-ID-RANGE>] [includes <REGEX>]  
[severity <COMPARISON-OPERATOR> <LEVEL>]
```

```
no <SEQUENCE-ID>
```

```
resequence <OLD-SEQUENCE-ID> <NEW-SEQUENCE-ID>
```

```
no logging filter <FILTER-NAME>
```

Description

Creates a filter to restrict what event or debug logs are logged. A filter can be used to either permit or deny:

- The event logs from being generated on the switch, or
- The event or debug logs generated on the switch from being forwarded to a syslog server.

A filter is identified by a filter name and can have up to 20 rules or entries, each with a different sequence number, matching criteria, and corresponding action (deny or permit). When a filter is applied on a log, the log is matched against the criteria mentioned in the rules or entries in ascending numerical order of their sequence numbers until a matching entry is found. Once a matching entry is found, its corresponding action is applied on the log. If no matching rule is found, the default action (permit) is applied.

The **no** form of this command removes the filter.

Parameter	Description
<FILTER-NAME>	Specifies the unique name to identify the filter.

Parameter	Description
enable	Filter event logs generated on the switch.
<SEQUENCE-ID>	Specifies the filter criteria sequence number. Default: Increments by 10 from the largest sequence-id currently used in this filter.
deny	Prevents the matching log from being logged.
permit	Allows the matching log.
<event-id>	Matches logs by event ID. Specify an event ID or a range of event IDs. It supports a maximum of 100 event IDs.
includes <REGEX>	Matches the log message against a regular expression string.
severity	Matches the logs by severity level. The following options are used to compare the severity: ▪ eq: Match events of severity equal to the specified. ▪ ge: Match events of severity greater than or equal to the specified. ▪ gt: Match events of severity greater than the specified. ▪ le: Match events of severity lesser than or equal to the specified. ▪ lt: Match events of severity lesser than the specified. The following are the severity levels: ▪ alert: Logs with the severity alert (6). ▪ crit: Logs with the severity critical (5). ▪ debug: Logs with the severity debug (0). ▪ emerg: Logs with the severity emergency (7). ▪ err: Logs with the severity err (4). ▪ info: Logs with the severity info (1). ▪ notice: Logs with the severity notice (2). ▪ warning: Logs with the severity warning (3).

Usage

Filtering event logs on the switch: To permit or deny event logs from being generated on the switch. In this case, the matching event logs are filtered at generation. The denied event logs are neither logged to the switch events nor forwarded to any remote syslog servers. Multiple filters can be configured, but only one filter can be applied to filter the events on the switch. Such a filter can be chosen by adding the **enable** command under its configuration. Configuring the **enable** command under a new filter automatically removes it from the filter where it was previously used.

For example:

```
logging filter low_severity_logs
enable
10 deny severity lt info
```

This configuration denies the event logs which have a severity less than info.



If a filter contains **enable** command, it is not recommended to configure this filter in the **logging** command used for remote syslog server configuration. This is because, any event logs denied by the filter are already not available for forwarding to a remote server.

A filter with **enable** command will not affect debug logs. Consider the configuration in the following example of a filter with **enable** command and two rules applied **10 permit severity ge info** and **20 deny**. This implies permit only those event logs which have severity greater than or equal to **info**.

Example:

```
logging filter low_severity_logs
enable
10 permit severity ge info
20 deny
```

Filtering event or debug logs when forwarding to a remote syslog server: The filter name must be configured in the logging command that is used to configure remote syslog server. The logs will be generated on the switch and the filter only decides whether to deny or permit the syslog forwarding for the matching log. For example: **logging 10.0.10.6 filter filter_ldap_logs**



The filter affects debug logs only when the command **debug destination syslog** is configured on the switch.

The severity mentioned in the remote syslog server configuration using logging command under configuration context has more precedence than the severity mentioned in a filter entry. If a log with **warning** severity is permitted by a filter, but the remote syslog configuration has severity **err** mentioned in it, the log will not be forwarded to the remote syslog server (since warning(3) is lesser than err(4)). On the other hand, if a log with **err** severity is permitted by a filter and the remote syslog configuration has severity **warning** mentioned in it, the log will be forwarded to the remote syslog server.



Examples

Configuring a new logging filter:

```
switch(config)# logging filter example_filter
```

To deny logs having event ID 1301 and a range of event IDs from 1305 to 1309:

```
switch(config-logging-filter)# 20 deny event-id 1301,1305-1309
```

To permit logs having event ID 1300:

```
switch(config-logging-filter)# 30 permit event-id 1300
```

To permit logs with severity greater than or equal to **err**:

```
switch(config-logging-filter)# 30 permit severity ge err
```

To deny logs with severity greater than info:

```
switch(config-logging-filter)# 30 deny severity gt info
```

To deny logs with event ID 1024 and a message matching the regular expression LLDP:

```
switch(config-logging-filter)# 40 deny event-id 1024 includes LLDP
```

Denying all logs:

```
switch(config-logging-filter)# 40 deny
```

Changing the sequence ID of an existing rule:

```
switch(config-logging-filter)# resequence 20 70
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config and config-logging-filter	Administrators or local user group members with execution rights for this command.

logging facility

```
logging facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}  
no logging facility
```

Description

Sets the logging facility to be used for remote syslog messages. Default: `local7`

The **no** form of this command disables the logging facility to be used for remote syslog messages.

Parameter	Description
{local0 local1 local2 local3 local4 local5 local6 local7}	Selects the logging facility to be used for remote syslog messages. Required. Specifies the severity of the syslog messages:

Parameter	Description
	▪ local0 ▪ local1 ▪ local2 ▪ local3 ▪ local4 ▪ local5 ▪ local6 ▪ local7

Examples

Sets the local5 logging facility to be used for remote syslog messages:

```
switch(config)# logging facility local5
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

logging persistent-storage

```
logging persistent-storage [severity {alert|crit|debug|emerg|err|info|notice|warning}]
no logging persistent-storage
```

Description

Enables or disables storage of logs in storage. Only logs of the specified severity and above will be preserved in the storage.

The **no** form of this command disables storage of logs in storage.



This command is deprecated. Please use "diag persistent-storage" command to preserve logs in storage.

Parameter	Description
<code>severity <LEVEL></code>	Specifies the severity of the syslog messages: ▪ alert: Preserves syslog messages with the severity of alert (6) and emergency (7) ▪ crit: Preserves syslog messages with the severity of critical (5) and above. Default. ▪ debug: Preserves syslog messages with the severity of debug (0) and above. ▪ emerg: Preserves syslog messages with the severity of emergency (7) only. ▪ err: Preserves syslog messages with the severity of err (4) and above. ▪ info: Preserves syslog messages with the severity of info (1) and above. ▪ notice: Preserves syslog messages with the severity of notice (2) and above. ▪ warning: Preserves syslog messages with the severity of warning (3) and above.

Usage

These logs can be copied out by using the **copy support-files all** or **copy support-files previous-boot**.

Examples

Enabling storage of logs in storage with severity **info**:

```
switch(config)#logging persistent-storage severity info
Logs will be written to storage and made available across reboot.
Do you want to continue (y/n)?
```

Disabling storage of logs in storage:

```
switch(config)# no logging persistent-storage
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.17	Command deprecated.
10.07 or earlier	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

Configuration commands

router rip

```
router rip <PROCESS-ID> [vrf <VRF-NAME>]  
no router rip <PROCESS-ID> [vrf <VRF-NAME>]
```

Description

Creates RIP process if not already created and enters the **router rip <PROCESS-ID>** context for the VRF mentioned. If no VRF is mentioned, a default is used. Only one RIP process is allowed per VRF.

The **no** form of this command deletes the RIP instance for the VRF. If no VRF is mentioned the default is deleted.

Parameter	Description
<PROCESS-ID>	Specifies name of the RIP process ID. Range: 1-63.
vrf <VRF-NAME>	Specifies VRF name.

Examples

Creating RIP process and naming the VRF:

```
switch(config)# router rip 2 vrf red
```

Deleting RIP process:

```
switch(config)# no router rip 2 vrf red
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

Interface commands

ip rip

```
ip rip <PROCESS-ID> {all-ip | ip-address}
no ip rip <PROCESS-ID> {all-ip | ip-address}
```

Description

Enables RIP process on an interface.

The **no** form of this command deletes the RIP process from an interface.

Parameter	Description
ip rip <PROCESS-ID>	Specifies RIP process ID. Range: 1-63.
all-ip	Specifies RIP for all IP addresses configured on the interface.
ip-address	Specifies IP address for RIP on the interface.

Usage

- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.
- If **ip rip 1 all-ip** is configured and a new IP address is added to the interface, RIP configurations will not be applicable for the newly added IP address.

Examples

Configuring RIP for all IP addresses configured on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 all-ip
```

Deleting RIP for all IP addresses configured on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip rip 1 all-ip
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip rip all-ip enable

```
ip rip all-ip enable
no ip rip all-ip enable
```

Description

Enables RIP process for all RIP enabled IP addresses configured on interface. The **no** form of this command disables RIP process on the interface.

Usage

- Default settings allow an interface to receive RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Enabling RIP process for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip all-ip enable
```

Disabling RIP process on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip rip all-ip enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip rip all-ip disable

```
ip rip all-ip disable
no ip rip all-ip disable
```

Description

Disables RIP process for all RIP enabled IP addresses configured on the interface.

The **no** form of this command enables RIP process for all RIP enabled IP addresses configured on the interface.

Usage

- Default settings allow an interface to receive RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Disabling RIP process for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip all-ip enable
```

Enabling RIP process for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip rip all-ip enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip rip all-ip send disable

```
ip rip all-ip send disable
no ip rip all-ip send disable
```

Description

Disables interface from sending RIP packets for all RIP enabled IP addresses.

The **no** form of this command enables interface to send RIP packets for all RIP enabled IP addresses.

Usage

- Default settings allow an interface to send RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Disabling interface from sending RIP packets for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip all-ip send disable
```

Enabling interface to send RIP packets for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip rip all-ip send disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

ip rip all-ip receive disable

```
ip rip all-ip receive disable
no ip rip all-ip receive disable
```

Description

Disables interface from receiving RIP packets for all enabled IP addresses.

The **no** form of this command enables interface to receive RIP packets for all RIP enabled IP addresses.

Usage

- Default settings allow an interface to receive RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Disabling interface from receiving RIP packets for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip all-ip receive disable
```

Enabling interface to receive RIP packets for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip rip all-ip receive disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

Routing commands

enable

enable
no enable

Description

Enables RIP process if disabled. By default RIP process is enabled.
The **no** form of this command disables the RIP process.

Examples

Enabling RIP process when disabled:

```
switch(config)# router rip 1
switch(config-rip-1)# enable
```

Disabling RIP process when enabled:

```
switch(config)# router rip 1  
switch(config-rip-1)# no enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

disable

disable
no disable

Description

Disables RIP process.

The **no** form of this command enables the RIP process.

Examples

Disabling RIP process:

```
switch(config)# router rip 1  
switch(config-rip-1)# disable
```

Enabling RIP process:

```
switch(config)# router rip 1  
switch(config-rip-1)# no disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

distance

distance <DISTANCE>
no distance

Description

Configures administrative distance for RIP. Administrative distance is used as criteria to select the best route when multiple protocols have the same route.

The **no** form of this command sets the RIP administrative distance to the default. Default: 120.

Parameter	Description
<DISTANCE>	Specifies RIP administrative distance. Range: 1 to 255.

Examples

Configuring administrative distance for RIP:

```
switch(config)# router rip 1  
switch(config-rip-1)# distance 100
```

Setting administrative distance for RIP to default values:

```
switch(config)# router rip 1  
switch(config-rip-1)# no distance
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

maximum-paths

```
maximum-paths <MAX-VALUE>
no maximum-paths
```

Description

Sets the maximum number of ECMP routes that RIP can support.

The **no** form of this command sets the maximum number of ECMP routes to the default value of 4.

Parameter	Description
<MAX-VALUE>	Sets the number of RIP ECMP routes. Range: 1-8.

Examples

Setting maximum number of RIP ECMP routes:

```
switch(config)# router rip 1
switch (config-rip-1)# maximum-paths 8
```

Setting maximum number of RIP ECMP routes to default:

```
switch(config)# router rip 1
switch (config-rip-1)# no maximum-paths
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute {bgp | connected | ospf <PROCESS-ID> | static}
no redistribute {bgp | connected | ospf <PROCESS-ID> | static}
```

Description

Redistributes routes originating from other protocols into RIP.

The **no** form of this command disables redistribution of routes originating from other protocols into RIP.

Parameter	Description
bgp	Specifies BGP routes to redistribute into RIP.
connected	Specifies connected routes (directly attached subnet or host) to redistribute into RIP.
ospf <PROCESS-ID>	Specifies the OSPF route to redistribute into RIP. Range: <1-65535>
static	Specifies static route to redistribute into RIP.



Parameters **ospf** and **bgp** are not supported on 6100 switches.

Examples

Redistributing BGP routes into RIP:

```
switch(config)# router rip 1
switch(config-rip-1)# redistribute bgp
```

Disabling BGP routes that originate from other protocols and redistribute into RIP:

```
switch(config)# router rip 1
switch(config-rip-1)# no redistribute bgp
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

timers update

```
timers update <INTERVAL> timeout <DURATION> garbage-collection <PERIOD>
no timers
```

Description

Configures RIP timers with specific values.

The **no** form of this command sets all RIP timers to default values.

Parameter	Description
<code>timers update <INTERVAL></code>	Specifies frequency at which RIP sends updates to all of its peers. Range: 1 to 2147484. Default: 30.
<code>timeout <DURATION></code>	Specifies timeout duration from the point of the last refresh after a route is received from a peer timeout and is marked as expired. Range: 1 to 255. Default: 180.
<code>garbage-collection <PERIOD></code>	Specifies amount of time route remains in routing table after route expiration. Range: 1 to 255. Default: 120.

Examples

Configuring RIP timers with specific values:

```
switch(config)# router rip 1  
switch(config-rip-1)# timers update 40 timeout 200 garbage-collection 150
```

Configuring RIP timers with default values:

```
switch(config)# router rip 1  
switch(config-rip-1)# no timers
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

RIPv2 clear commands

clear ip rip statistics

```
clear ip rip [<PROCESS-ID>] statistics [all-vrfs | vrf <VRF-NAME>]
```

Description

Clears RIP event statistics.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID. Range: 1-63
all-vrfs	Clears statistics for all VRFs.
vrf	Selects VRF to clear statistics for.
<VRF-NAME>	Specifies VRF name.

Examples

Clearing RIP event statistics:

```
switch# clear ip rip statistics
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

RIPv2 interface commands

enable

enable
no enable

Description

Enables RIP process for RIP enabled IP address configured on interface.

The **no** form of this command disables RIP process on interface.

Usage

- Default settings allow an interface to receive RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Enabling RIP process for RIP enabled IP address:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# enable
```

Disabling RIP process on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# no enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

disable

disable
no disable

Description

Disables RIP process for RIP enabled IP addresses configured on interface.
The **no** form of this command enables RIP process on interface.

Examples

Disabling RIP process for RIP enabled IP addresses configured on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# disable
```

Enabling RIP process on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# no disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

send disable

send disable
no send disable

Description

Disables an interface from sending RIP packets for a specific IP address.

The **no** form of this command enables interface for sending RIP packets for a specific IP address.

Usage

- Default settings allow an interface to send and receive RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Disabling interface from sending RIP packets for a specific IP address :

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# send disable
```

Enabling interface to send RIP packets for a specific IP address:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# no send disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

receive disable

```
receive disable
no receive disable
```

Description

Disables interface from receiving RIP packets for a specific IP address.

The **no** form of this command enables interface for receiving RIP packets for a specific IP address.

Usage

- Default settings allow an interface to receive RIP packets.
- If an IP address is removed from an interface configured with RIP, all RIP configurations will be removed from the interface.

Examples

Disabling interface from receiving RIP packets for a specific IP address:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# receive disable
```

Enabling interface for receiving RIP packets for a specific IP address:

```
switch(config)# interface 1/1/1
switch(config-if)# ip rip 1 10.1.1.1
switch(config-if-rip)# no receive disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

RIPv2 show commands

show capacities rip

show capacities rip

Description

Displays maximum number of RIP interfaces, routes and process.

Examples

Displaying maximum number of RIP interfaces, routes and process:

```
switch# show capacities rip

System Capacities: Filter RIP
Capacities Name                                     Value
-----
Maximum number of RIP interfaces configurable in the system      32
Maximum number of RIP processes supported across each VRF        1
Maximum number of routes in RIP supported across all VRFs       2540
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show capacities-status rip

show capacities-status rip

Description

Displays number of RIP interfaces, routes and process configured in the system.

Examples

Displaying number of RIP interfaces, routes and process:

```
switch# show capacities-status rip

System Capacities Status: Filter RIP
Capacities Name                                     Value Maximum
-----
```

Number of RIP interfaces configured in the system	0	32



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ip rip

show ip rip [<PROCESS-ID>] [all-vrfs | vrf <VRF-NAME>]

Description

Displays general RIP configuration.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID. Range: 1-63.
all vrfs	Displays general RIP information for all VRFs.
vrf	Selects VRF to display general RIP information for.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters display general RIP information for a specific RIP process.
- Parameters display general RIP information for a specific or all VRFs.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying general RIP configuration for all VRFs:

```
switch# show ip rip 34 all-vrfs
VRF : Default                      Process-ID : 34
-----
RIP Version           : RIPv2      Protocol Status : Enabled
```

```
Update Time           : 60 sec   Timeout Time        : 240 sec
Garbage Collection Time : 250 sec ECMP                     : 6
Distance              : 100      Redistribution          : static,
                                   ospf 1
```

```
VRF : vrf_1                      Process-ID : 34
```

```
-----
RIP Version           : RIPv2    Protocol Status      : Enabled
Update Time          : 30 sec   Timeout Time         : 180 sec
Garbage Collection Time : 120 sec ECMP                     : 4
Distance             : 120      Redistribution          : None
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ip rip interface

```
show ip rip [<PROCESS-ID>] interface [<INTERFACE-NAME>] [brief] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays information about RIP enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID. Range: 1-63.
<INTERFACE-NAME>	Specifies interface.
brief	Shows brief overview information for the RIP interface.
all-vrfs	Displays interface information for all VRFs.
vrf	Selects specific VRF.
<VRF-NAME>	Specifies VRF.

Usage

- Parameters display general RIP information for a specific RIP process.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

```
switch# show ip rip interface
Interface 1/1/1 is up, IP Address is 10.10.10.1/24
-----
VRF           : Default           Process-ID    : 1
Status        : Oper Up           Mode          : Send and Receive
MTU           : 500               Version       : RIPv2
Poision Reverse : Enabled

Interface 1/1/2 is up, IP Address is 20.10.10.1/24
-----
VRF           : Default           Process-ID    : 1
Status        : Admin Down        Mode          : Receive
MTU           : 500               Version       : RIPv2
Poision Reverse : Enabled

Interface 1/1/3 is up, IP Address is 30.10.10.1/24
-----
VRF           : Default           Process-ID    : 1
Status        : Admin Down        Mode          : Send
MTU           : 500               Version       : RIPv2
Poision Reverse : Enabled

switch# show ip rip interface brief
VRF : default   Process-ID : 1
-----

Total Number of Interfaces: 2

Interface      IP-Address/Mask      Status      MTU
-----
1/1/1          10.10.10.1/24        up          500
1/1/2          20.10.10.1/24        up          500
1/1/3          30.10.10.1/24        up          500
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ip rip neighbors

```
show ip rip [<PROCESS-ID>] neighbors [<IP-ADDRESS>] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays information about RIP neighbors.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID. Range: 1-63.
<IP-ADDRESS>	Specifies IP address of a specific neighbor to display information on.
all-vrfs	Displays neighbor information for all VRFs.
vrf	Selects VRF to display neighbor information.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters display RIP neighbor information for a specific RIP process.
- Parameters display RIP neighbor information for a specific neighbor.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIP neighbor information for all VRFs:

```
switch# show ip rip neighbors all-vrfs
VRF : default          Process-ID : 1
-----

Total Number of Neighbors: 1

Peer-Address    Type      Last-Update  Rcvd-Bad-Pkts  Rcvd-Bad-Routes
-----
1.1.1.2         RIPv2     0:0:7        4               5
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ip rip routes

show ip rip [<PROCESS-ID>] routes [<PREFIX/LENGTH>] [all-vrfs | vrf <VRF-NAME>]

Description

Displays RIP routing table for a specific RIP process.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID to display information for a specific RIP process. Range: 1-63.
<PREFIX/LENGTH>	Specifies the network prefix.
all-vrfs	Displays RIP routing information for all VRFs.
vrf	Selects VRF to display RIP routing information.
<VRF-NAME>	Specifies VRF name.

Usage

- <PREFIX/LENGTH> is an optional parameter that displays RIP routing table information for a specific subnet.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIP routing table for all VRFs:

```
switch# show ip rip routes all-vrfs
VRF : default          Process-ID : 1
-----
Total Number of Routes : 6

Prefix          Metric    Interface    Nexthop
-----
10.1.0.0/16      2         1/1/1        30.1.1.2
20.1.2.0/24      3         1/1/1        30.1.1.2
30.1.1.0/24      1         1/1/1

VRF : vrf_1          Process-ID : 34
-----

Prefix          Metric    Interface    Nexthop
-----
20.1.0.0/16      10        1/1/2        50.1.1.2
40.1.2.0/24      14        1/1/2        50.1.1.2
50.1.1.0/24      1         1/1/2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ip rip statistics

show ip rip [<PROCESS-ID>] statistics [all-vrfs | vrf <VRF-NAME>]

Description

Displays RIP statistics.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID. Range: 1-63.
all-vrfs	Displays statistics information for all VRFs.
vrf	Selects VRF to display RIP statistics information for.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters can display information for all VRFs or a specific VRF.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIP statistics for all VRFs:

```
switch# show ip rip statistics all-vrfs
VRF : default  Process-ID : 1
-----

Global Route Changes : 50
Global Queries       : 2
Last Cleared          : 0h 30m 28s ago

VRF : vrf_1      Process-ID : 34
-----

Global Route Changes : 20
Global Queries       : 0
Last Cleared          : 0h 30m 28s ago
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ip rip statistics interface

show ip rip [<PROCESS-ID>] statistics interface [<INTERFACE-NAME>] [all-vrfs | vrf <VRF-NAME>]

Description

Displays RIP statistics for RIP enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies RIP process ID. Range: 1-63.
<INTERFACE-NAME>	Specifies name of interface.
all-vrfs	Displays RIP interface statistics for all VRFs.
vrf	Selects VRF to display RIP interface statistics.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters can display information for all VRFs or a specific VRF.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIP statistics for a RIP enabled interface:

```
switch# show ip rip statistics interface 1/1/1
VRF : default Process-ID : 1 interface 1/1/1
-----
IP-Address    Trigger-Updates    Rcvd-Bad-Packets    Rcvd-Bad-Routes
-----
10.1.1.1      15                  3                    4
Last Cleared : 0h 30m 28s ago
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show running-config

show running config

Description

Displays all running configurations for all protocols including RIP.

Examples

Displaying all running configurations for all protocols including RIP:

```
switch# show running-config
Current configuration:
!
!Version Halon 0.1.0 (Build: genericx86-64-Halon-0.1.0-master-20170309054955-dev)
!Schema version 0.1.8
lldp enable
timezone set utc
vrf blue
vrf green
vrf red
led base-loc_fdc on
led base-loc on
led base-hlth_fdc fast_blink
led base-pwr_fdc on
!
!
!
!
!
!
aaa authentication login default local
aaa authorization commands default none
!
!
!
!
router ospf 1 vrf red
router rip 1
    maximum-paths 5
    distance 1
router rip 1 vrf red
    default-information originate always
    maximum-paths 7
```

```

distance 5
redistribute ospf 1
timers update 40 timeout 200 garbage-collection 120
vlan 1
  no shutdown
interface lag 44
  no shutdown
  ip address 33.1.1.1/24
  ip rip 1 33.1.1.1
    send disable
interface 1/1/1
  no shutdown
  ip address 33.44.1.1/24
  ip address 44.44.1.1/24 secondary
  ip rip 1 33.44.1.1
    send disable
  ip rip 1 44.44.1.1
    send disable
interface 1/1/2
interface loopback 2
  ip address 55.55.55.55/32
  ip rip 1 55.55.55.55

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

Configuration commands

router ripng

```
router ripng <PROCESS-ID> [vrf <VRF-NAME>]  
no router ripng <PROCESS-ID> [vrf <VRF-NAME>]
```

Description

Creates RIPng process if not already created and enters the **router ripng <PROCESS-ID>** context for the VRF mentioned. If no VRF is mentioned, a default is used. Only one RIPng process is allowed per VRF.

The **no** form of this command deletes the RIPng instance for the VRF. If no VRF is mentioned the default is deleted.

Parameter	Description
<PROCESS-ID>	Specifies name of the RIPng process ID. Range: <1-63>
vrf	Sets VRF name for RIPng process.
<VRF-NAME>	VRF name for VRF.

Examples

Creating RIPng process and naming the VRF:

```
switch(config)# router ripng 2 vrf red
```

Deleting RIPng process:

```
switch(config)# no router ripng 2 vrf red
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

Interface commands

ipv6 ripng

```
ipv6 ripng <PROCESS-ID>
no ipv6 ripng <PROCESS-ID>
```

Description

Enables RIPng process on interface and creates a new context.
The **no** form of this command deletes RIPng process on interface.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63.

Examples

Enabling RIPng process on an interface:

```
switch(config)# interface 1/1/1
switch (config-if)# ipv6 ripng 1
switch (config-if-ripng)#
```

Deleting RIPng process on an interface:

```
switch(config)# interface 1/1/1
switch (config-if)# no ipv6 ripng 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

Routing commands

enable

enable
no enable

Description

Enables RIPng process if disabled. By default RIPng process is enabled.
The **no** form of this command disables the RIPng process.

Examples

Enabling RIPng process when disabled:

```
switch(config) # router ripng 1  
switch(config-ripng-1) # enable
```

Disabling RIPng process when enabled:

```
switch(config) # router ripng 1  
switch(config-ripng-1) # no enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

disable

disable
no disable

Description

Disables RIPng process.
The **no** form of this command enables the RIPng process.

Examples

Disabling RIPng process:

```
switch(config)# router ripng 1  
switch(config-ripng-1)# disable
```

Enabling RIPng process:

```
switch(config)# router ripng 1  
switch(config-ripng-1)# no disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

distance

distance <DISTANCE>
no distance

Description

Configures administrative distance for RIPng. Administrative distance is used as criteria to select the best route when multiple protocols have the same route.

The **no** form of this command sets the RIPng administrative distance to the default. Default: 120.

Parameter	Description
<DISTANCE>	Specifies RIPng administrative distance. Range: 1 to 255.

Examples

Configuring administrative distance for RIPng:

```
switch(config)# router ripng 1  
switch(config-ripng-1)# distance 100
```

Setting administrative distance for RIPng to default values:

```
switch(config)# router ripng 1  
switch(config-ripng-1)# no distance
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

maximum-paths

maximum-paths <MAX-VALUE>
no maximum-paths

Description

Sets the maximum number of ECMP routes that RIPng can support.

The **no** form of this command sets the maximum number of ECMP routes to the default value of 4.

Parameter	Description
<MAX-VALUE>	Sets the number of RIPng ECMP routes. Range: 1-8.

Examples

Setting maximum number of RIPng ECMP routes:

```
switch(config)# router ripng 1
switch (config-ripng-1)# maximum-paths 8
```

Setting maximum number of RIPng ECMP routes to default:

```
switch(config)# router ripng 1
switch (config-ripng-1)# no maximum-paths
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

redistribute

```
redistribute {bgp | connected | ospfv3 <PROCESS-ID> | static}  
no redistribute {bgp | connected | ospfv3 <PROCESS-ID> | static}
```

Description

Redistributes routes originating from other protocols into RIPng.

The **no** form of this command disables redistribution of routes originating from other protocols into RIPng.

Parameter	Description
bgp	Specifies BGP routes to redistribute into RIPng.
connected	Specifies connected routes (directly attached subnet or host) to redistribute into RIPng.
ospfv3 <PROCESS-ID>	Specifies the OSPFv3 route to redistribute into RIPng. Range: <1-65535>
static	Specifies static route to redistribute into RIPng.



Parameters **ospfv3** and **bgp** are not supported on 6100 switches.

Examples

Redistributing BGP routes into RIPng:

```
switch(config)# router ripng 1  
switch(config-ripng-1)# redistribute bgp
```

Disabling BGP routes that originate from other protocols and redistribute into RIPng:

```
switch(config)# router ripng 1  
switch(config-ripng-1)# no redistribute bgp
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.14	Supported process ID range expanded from 1-63 to 1-65535.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

timers update

timers update <INTERVAL> timeout <DURATION> garbage-collection <PERIOD>
no timers

Description

Configures RIPng timers with specific values.

The **no** form of this command sets all RIPng timers to default values.

Parameter	Description
timers update <INTERVAL>	Specifies frequency at which RIPng sends updates to all of its peers. Range: 1 to 2147484. Default: 30.
timeout <DURATION>	Specifies timeout duration from the point of the last refresh after a route is received from a peer timeout and is marked as expired. Range: 1 to 255. Default: 180.
garbage-collection <PERIOD>	Specifies amount of time route remains in routing table after route expiration. Range: 1 to 255. Default: 120.

Examples

Configuring RIPng timers with specific values:

```
switch(config)# router ripng 1
switch(config-ripng-1)# timers update 40 timeout 200 garbage-collection 150
```

Configuring RIPng timers with default values:

```
switch(config)# router ripng 1
switch(config-ripng-1)# no timers
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

RIPng clear commands

clear ipv6 ripng statistics

```
clear ipv6 ripng [<PROCESS-ID>] statistics [all-vrfs | vrf <VRF-NAME>]
```

Description

Clears RIPng event statistics.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63
all-vrfs	Clears statistics for all VRFs.
vrf	Selects VRF to clear statistics for.
<VRF-NAME>	Specifies VRF name.

Examples

Clearing RIPng event statistics:

```
switch# clear ipv6 ripng statistics
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

RIPng interface commands

enable

enable
no enable

Description

Enables RIPng process on interface.

The **no** form of this command disables RIPng process on interface.

Examples

Enabling RIPng process on interface:

```
switch(config) # interface 1/1/1
switch(config-if) # ipv6 ripng 1
switch(config-if-ripng) # enable
```

Disabling RIPng process on interface:

```
switch(config) # interface 1/1/1
switch(config-if) # ipv6 ripng 1
switch(config-if-ripng) # no enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

disable

disable
no disable

Description

Disables RIPng process on interface.

The **no** form of this command enables RIPng process on interface.

Examples

Disabling RIP process for all RIP enabled IP addresses on interface:


```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 ripng 1
switch(config-if-ripng)# disable
```

Enabling RIP process for all RIP enabled IP addresses on interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 ripng 1
switch(config-if-ripng)# no disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

send disable

send disable
no send disable

Description

Disables interface from sending RIPng packets. An interface can send RIPng packets by default. The **no** form of this command enables interface to send RIPng packets, if disabled.

Examples

Disabling interface from sending RIPng packets:

```
switch(config)# interface 1/1/1
switch (config-if)# ipv6 ripng 1
switch (config-if-ripng)# send disable
```

Enabling interface to send RIPng packets:

```
switch(config)# interface 1/1/1
switch (config-if)# ipv6 ripng 1
switch (config-if-ripng)# no send disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

receive disable

receive disable
no receive disable

Description

Disables interface from receiving RIPng packets for all enabled IP addresses. An interface can receive RIPng packets by default.

The **no** form of this command enables interface to receive RIPng packets, if disabled.

Examples

Disabling interface from receiving RIPng packets:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 ripng 1
switch (config-if-ripng)# receive disable
```

Enabling interface to receive RIPng packets when disabled:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 ripng 1
switch (config-if-ripng)# no receive disable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-if	Administrators or local user group members with execution rights for this command.

RIPng show commands

show capacities ripng

show capacities ripng

Description

Displays the maximum number of RIPng interfaces, routes and process.

Examples

Displaying maximum number of RIPng interfaces, routes and process:

```
switch# show capacities ripng

System Capacities: Filter RIPng
Capacities Name                                     Value
-----
Maximum number of RIPng interfaces configurable in the system 32
Maximum number of RIPng processes supported across each VRF    1
Maximum number of routes in RIPng supported across all VRFs    2540
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show capacities-status ripng

show capacities-status ripng

Description

Displays number of RIPng interfaces, routes and process configured in the system.

Examples

Displaying number of RIPng interfaces, routes and process:

```
switch# show capacities-status ripng

System Capacities Status: Filter RIPng
```

Capacities Name	Value	Maximum

Number of RIPng interfaces configured in the system	0	32



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ipv6 ripng

show ipv6 ripng [<PROCESS-ID>] [all-vrfs | vrf <VRF-NAME>]

Description

Displays general RIPng configuration.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63.
all vrfs	Displays general RIPng information for all VRFs.
vrf	Selects VRF to display general RIPng information for.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters display general RIPng information for a specific RIPng process.
- Parameters display general RIPng information for a specific or all VRFs.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying general RIPng configuration for all VRFs:

```

switch# show ipv6 ripng 34 all-vrfs
VRF : Default                               Process-ID : 34
-----
Protocol Status      : Enabled    ECMP           : 6
Update Time         : 60 sec     Timeout Time    : 240 sec
Garbage Collection Time : 250 sec Distance         : 100
Redistribution       : static,
                    ospfv3 1

VRF : vrf_1                               Process-ID : 34
-----
Protocol Status      : Enabled    ECMP           : 4
Update Time         : 30 sec     Timeout Time    : 180 sec
Garbage Collection Time : 120 sec Distance         : 120
Redistribution       : None

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ipv6 ripng interface

show ipv6 ripng [<PROCESS-ID>] interface [<INTERFACE-NAME>] [brief] [all-vrfs | vrf <VRF-NAME>]

Description

Displays information about RIPng enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63.
<INTERFACE-NAME>	Specifies interface.
brief	Shows brief overview information for RIPng interface.
all-vrfs	Displays interface information for all VRFs.
vrf	Selects specific VRF.
<VRF-NAME>	Specifies VRF.

Usage

- Parameters display general RIPng information for a specific RIPng process.
- Parameters display general RIPng information for a specific or all VRFs.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

```
switch# show ipv6 ripng interface
Interface 1/1/1 is up, IPv6 Address is fe80::7272:cfff:fe70:67a
-----
VRF           : Default           Process-ID    : 1
Status        : Oper Up           Mode          : Send and Receive
MTU           : 500               Poision Reverse : Enabled

Interface 1/1/2 is up, IPv6 Address is fe80::7272:cfff:fe70:67a
-----
VRF           : Default           Process-ID    : 1
Status        : Admin Down        Mode          : Receive
MTU           : 500               Poision Reverse : Enabled

Interface 1/1/3 is up, IPv6 Address is fe80::7272:cfff:fe70:67a
-----
VRF           : Default           Process-ID    : 1
Status        : Admin Down        Mode          : Send
MTU           : 500               Poision Reverse : Enabled

switch# show ipv6 ripng interface brief
VRF : default   Process-ID : 1
-----

Total Number of Interfaces: 2

Interface      IPv6-Address          Status    MTU
-----
1/1/1         fe80::7272:cfff:fe70:67a    up        500
1/1/2         fe80::7272:cfff:fe71:67a    up        500
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ipv6 ripng neighbors

```
show ipv6 ripng [<PROCESS-ID>] neighbors [<LINK-LOCAL-ADDRESS>] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays information about RIPng neighbors.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63.
neighbors	Specifies neighbor IP address.
<LINK-LOCAL-ADDRESS>	Specifies link-local address.
all-vrfs	Displays neighbor information for all VRFs.
vrf	Selects VRF to display neighbor information.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters display RIPng neighbor information for a specific RIPng process.
- Parameters display RIPng neighbor information for a specific neighbor.
- Parameters display general RIPng information for a specific or all VRFs.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIPng neighbor information for all VRFs:

```
switch# show ipv6 ripng neighbors all-vrfs
VRF : default          Process-ID : 1
-----

Total Number of Neighbors: 1

Peer-Address      Type      Last-Update  Rcvd-Bad-Pkts  Rcvd-Bad-Routes
-----
fe80::7272:cfff:fe70:86ae
                  RIPng    0:0:7        4              5
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ipv6 ripng routes

show ipv6 ripng [<PROCESS-ID>] routes [<PREFIX/LENGTH>] [all-vrfs | vrf <VRF-NAME>]

Description

Displays RIPng routing table for a specific RIPng process.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID to display information for a specific RIPng process. Range: 1-63.
<PREFIX/LENGTH>	Specifies the network prefix.
all-vrfs	Displays RIPng routing information for all VRFs.
vrf	Selects VRF to display RIPng routing information.
<VRF-NAME>	Specifies VRF name.

Usage

- <PREFIX/LENGTH> is an optional parameter that displays RIPng routing table information for a specific subnet.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIPng routing table for all VRFs:

```
switch# show ipv6 ripng routes all-vrfs
VRF : default          Process-ID : 1
-----
Prefix                Metric    Interface    Nexthop
-----
2001:DB8:10::/64      2        1/1/1        FE80::2E0:E6FF:FE1B:8242
2002:DB8:10::/64      3        1/1/1        FE80::2E0:E6FF:FE1B:8242
2003:DB8:10::/64      1        1/1/1
VRF : vrf_1           Process-ID : 34
-----
Prefix                Metric    Interface    Nexthop
-----
3001:DB8:10::/64      10       1/1/2        FE80::2E0:E6FF:FE1B:8232
3002:DB8:10::/64      14       1/1/2        FE80::2E0:E6FF:FE1B:8232
3003:DB8:10::/64      1        1/1/2
```




For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ipv6 ripng statistics

show ipv6 ripng [<PROCESS-ID>] statistics [all-vrfs | vrf <VRF-NAME>]

Description

Displays RIPng statistics.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63.
all-vrfs	Displays statistics information for all VRFs.
vrf	Selects VRF and displays RIPng statistics for it.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters can display information for all VRFs or a specific VRF.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIPng statistics for all VRFs:

```
switch# show ipv6 ripng statistics all-vrfs
VRF : default  Process-ID : 1
-----

Global Route Changes : 50
Global Queries       : 2
Last Cleared         : 0h 30m 28s ago

VRF : vrf_1      Process-ID : 34
-----
```

```
Global Route Changes : 20
Global Queries       : 0
Last Cleared          : 0h 30m 28s ago
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ipv6 ripng statistics interface

```
show ipv6 ripng [<PROCESS-ID>] statistics interface [<INTERFACE-NAME>] [all-vrfs | vrf <VRF-NAME>]
```

Description

Displays RIPng statistics for RIPng enabled interfaces.

Parameter	Description
<PROCESS-ID>	Specifies RIPng process ID. Range: 1-63.
<INTERFACE-NAME>	Specifies name of interface.
all-vrfs	Displays RIPng interface statistics for all VRFs.
vrf	Selects VRF to display RIPng interface statistics.
<VRF-NAME>	Specifies VRF name.

Usage

- Parameters can display information for all VRFs or a specific VRF.
- If a VRF is not mentioned, information for the default VRF is displayed.

Examples

Displaying RIPng statistics for a RIPng enabled interface:

```
switch# show ipv6 ripng statistics interface 1/1/1
VRF : default Process-ID : 1 interface 1/1/1
```

```

-----
IPv6-Address      Trigger-Updates      Rcvd-Bad-Packets      Rcvd-Bad-Routes
-----
fe80::7272:cfff:fe70:86ae
                  15                      3                      4

Last Cleared: 0h 30m 28s ago

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show running-config

show running config

Description

Displays all running configurations for all protocols including RIPng.

Examples

Displaying all running configurations for all protocols including RIPng:

```

switch# show running-config
Current configuration:
!
!Version Halon 0.1.0 (Build: genericx86-64-Halon-0.1.0-master-20170309054955-dev)
!Schema version 0.1.8
lldp enable
timezone set utc
vrf green
vrf red
led base-loc_fdc on
led base-loc on
led base-hlth_fdc fast_blink
led base-pwr_fdc on
!
!
!
!
!

```

```

!
aaa authentication login default local
aaa authorization commands default none
!
!
!
!
router ospfv3 1
router ripng 1
    maximum-paths 5
    distance 1
    redistribute ospfv3 1
    timers update 40 timeout 200 garbage-collection 150
router ripng 1 vrf red
    default-information originate always
    maximum-paths 7
    distance 5
vlan 1
    no shutdown
interface lag 44
    no shutdown
    ipv6 address link-local
    ipv6 ripng 1
        send disable
interface 1
    no shutdown
    ipv6 address link-local
    ipv6 ripng 1
        receive disable

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

Route policy and route map commands

This section describes general and filtering commands, as well as match, set and show commands for configuring route policies and route maps.

General or filtering commands

ip aspath-list

```
ip aspath-list <ASPATH-LIST-NAME> [seq <SEQ>] {permit | deny} <REGEXP>  
no ip aspath-list <ASPATH-LIST-NAME> [seq <SEQ>] {permit | deny} <REGEXP>
```

Description

Configures an AS Path list to match a specific AS path. AS Path lists are named lists of regular expression rules. They are used to match AS Path attributes in the routes for inclusion in or exclusion from route policies. The sequence number is optional and is autogenerated whenever it is not explicitly mentioned. All AS Path list rules with the same name are grouped together.

The **no** form of this command removes the AS Path list configuration.

Parameter	Description
<ASPATH-LIST-NAME>	Specifies the name of the AS Path list.
seq <SEQ>	Specifies the order of reference of the regular expression rules.
{permit deny}	Specifies whether the route is available for further processing when there is a match.
<REGEXP>	Specifies the regular expression to match the AS Path. Standard regular expression wildcards are supported. The _ character can be used to match the AS Path boundary.

Examples

Configuring an AS Path list with sequence numbering:

```
switch(config)# ip aspath-list ASLst seq 5 permit _4*
```

Configuring a prefix list without sequence numbering:

```
switch(config)# ip aspath-list ASLst permit _4*
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ip community-list

```
ip community-list standard <COMM-LIST-NAME> <DESCRIPTION> [seq <SEQ>] {permit | deny}
<COMMUNITY-NUMBER>
no ip community-list standard <COMM-LIST-NAME> <DESCRIPTION> [seq <SEQ>] {permit | deny}
<COMMUNITY-NUMBER>
```

Description

Configures a community list to match a specific community number attribute. Community-list is a named list of regular expressions. They are used to match the community number attributes in the routes for inclusion in, or exclusion from route policies. The sequence number is optional and is autogenerated whenever it is not explicitly mentioned. All community-list rules with the same name are grouped.

The **no** form of this command removes the community list configuration.

Parameter	Description
<COMM-LIST-NAME>	Specifies the name of the community list that matches community number of a route.
<DESCRIPTION>	Specifies the description of the community list. Maximum character limit is 80.
seq <SEQ>	Specifies the order of reference of the regular expression rules.
{permit deny}	Specifies whether the route is available for further processing when there is a match.
<COMMUNITY-NUMBER>	Specifies the community number. The community number must be in AA: NN format or from the list of well-known community.

Examples

Configuring a community list with sequence numbering:

```
switch(config)# ip community-list standard CommList seq 5 permit 101:41
```

Configuring a community list without sequence numbering:

```
switch(config)# ip community-list standard CommList no-export permit
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ip prefix-list

```
ip prefix-list <PREFIX-LIST-NAME> [seq <SEQ>] <IP-PREFIX/MASK> [ge <0-32>] [le <0-32>]  
no ip prefix-list <PREFIX-LIST-NAME> [seq <SEQ>] <IP-PREFIX/MASK> [ge <0-32>] [le <0-32>]
```

Description

Configures a prefix list to match a set of prefixes. Prefix lists are named lists of route prefixes. They are used to match routes for inclusion in or exclusion from route policies. The sequence number determines the order of matching. The matches are performed starting from the lowest sequence number to the highest sequence number until there is a match. The sequence number is however optional and is autogenerated whenever it is not explicitly mentioned. All prefixes with the same prefix list name are grouped.

The autogenerated sequence number is derived by adding 10 to the highest sequence number available. This technique makes it possible to insert new prefix list sequence number in between.

The **ge** and **le** parameters are used to combine prefixes with a range of network mask. For example, **172.131.0.0/16 ge 16 le 24** will match all prefixes within the 172.131.0.0/16 network that have a mask greater than or equal to 16 bits and less than or equal to 24 bits in length. For instance, 172.131.1.0/18 would match, because its length is between 16 and 24 but 172.0.0.0/8 or 172.131.1.128/25 would not match.

The **no** form of this command removes the prefix list configuration. Prefix-list commands which generate sequence numbers must explicitly use sequence numbers in the **no** form.

Parameter	Description
<PREFIX-LIST-NAME>	Specifies the name of the prefix list.
seq <SEQ>	Specifies the order of reference of the prefix rules.
{permit deny}	Specifies whether the route is available for further processing when there is a match.
IP-PREFIX/MASK>	Specifies the IP prefix or mask.
ge <0-32>	Specifies the minimum prefix length to be matched.
le <0-32>	Specifies the maximum prefix length to be matched.

Examples

Configuring a prefix list with sequence numbering:

```
switch(config)# ip prefix-list PFXLST seq 5 permit 4.0.0.0/8 ge 9 le 12
```

Configuring a prefix list without sequence numbering:

```
switch(config)# ip prefix-list PSXLST permit 5.0.0.0/8
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ipv6 prefix-list

```
ipv6 prefix-list <PREFIX-LIST-NAME> [seq <SEQ>] <IPV6-PREFIX/MASK> [ge <0-128>] [le <0-128>]  
no ipv6 prefix-list <PREFIX-LIST-NAME> [seq <SEQ>] {ip | ipv6} <IPV6-PREFIX/MASK> [ge <0-128>] [le <0-128>]
```

Description

Configures a prefix list to match a set of prefixes. Prefix lists are named lists of route prefixes. They are used to match routes for inclusion in or exclusion from route policies. The sequence number determines the order of matching. The matches are performed starting from the lowest sequence number to the highest sequence number until there is a match. The sequence number is however optional and is autogenerated whenever it is not explicitly mentioned. All prefixes with the same prefix list name are grouped.

The autogenerated sequence number is derived by adding 10 to the highest sequence number available. This technique makes it possible to insert new prefix list sequence number in between.

The **ge** and **le** parameters are used to combine prefixes with a range of network mask. For example, **2000::/64 ge 65 le 70** will match all prefixes within the 2000::/64 network that have a mask greater than or equal to 65 bits and less than or equal to 70 bits in length.

The **no** form of this command removes the prefix list configuration. Prefix-list commands which generate sequence numbers must explicitly use sequence numbers in the **no** form.

Parameter	Description
<i><PREFIX-LIST-NAME></i>	Specifies the name of the prefix list.
seq <i><SEQ></i>	Specifies the order of reference of the prefix rules.
{permit deny}	Specifies whether the route is available for further processing when there is a match.
<i>IP-PREFIX/MASK></i>	Specifies the IP prefix or mask.
ge <i><0-128></i>	Specifies the minimum prefix length to be matched.
le <i><0-128></i>	Specifies the maximum prefix length to be matched.

Examples

Configuring a prefix list with sequence numbering:

```
switch(config)# ipv6 prefix-list PFXLST seq 10 permit 2000::64 ge 65 le 70
```

Configuring a prefix list without sequence numbering:

```
switch(config)# ipv6 prefix-list PSXLST permit 2000::1/128
```

Removing the configuring of a prefix list:

```
switch(config)# no ipv6 prefix-list P2 seq 10 permit any
```

Removing the configuring of a prefix list:

```
switch(config)# no ipv6 prefix-list P1 seq 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

route-map

```
route-map <NAME> {permit | deny} seq <NUMBER>
no route-map <NAME> {permit | deny} seq <NUMBER>
```

Description

Configures a route map entry with the given name and action by taking the CLI in the route map context. All route map entries with the same name belong to the same route map. The route map entry rules are processed in order by sequence number, until a match is found.

The **no** form of this command removes the route map entry configuration.

Parameter	Description
<NAME>	Specifies the name of the route map. Required.
{permit deny}	Specifies whether the route is available for further processing when there is a match. Required.
<NUMBER>	Specifies the sequence number of the entry. Required.

Examples

Configuring a route map entry:

```
switch(config)# route-map GlobalMap permit seq 10
```

Removing a route map entry configuration:

```
switch(config)# no route-map GlobalMap permit seq 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

continue

```
continue <SEQUENCE NUMBER>
no continue
```

Description

Allows you to execute additional entries in a route map. The sequence number specifies the route-map entry's sequence number that will be executed next if the existing entry's match clause is successful. If a successful match occurs and continue command exists, the route map saves the set value first and then jumps to the specified route map entry.

Set clauses are saved during the match clause evaluation and are executed only after the route map evaluation is completed. The set clauses are executed in the order in which they were configured.

Set clauses can be accumulative or additive as **set as-path prepend** or it can be absolute as **set metric**. For set commands that configures an accumulative value, subsequent values are added in order in which they were configured. For set commands that configures an absolute value, The values from the last instance will be applied.

The **no** form of this command removes the route map continue configuration.



If the specified route-map sequence entry does not exist, route-map processing will be terminated at the current sequence number if its clause is matched. The continue sequence number must be higher than the current route map sequence number for this command to take effect.

Parameter	Description
<code><SEQUENCE NUMBER></code>	Specifies the value of the route map entry to be executed next after a successful match clause.

Examples

Configuring a route map to continue to execute an additional entry:

```
switch(config)# route-map GlobalMap permit 10  
switch(config-route-map-GlobalMap-10)# continue 40
```

Removing a route map continue configuration:

```
switch(config)# route-map GlobalMap permit seq 10  
switch(config-route-map-GlobalMap-10)# no continue 40
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

Match commands

match aspath-list

```
match aspath-list <ASPATH-LIST-NAME>
no match aspath-list <ASPATH-LIST-NAME>
```

Description

Matches the AS path attribute of the route with one or more regular expressions in the AS path list.

The **no** form of this command restores the default behavior of not matching the AS path attribute of the route.

Parameter	Description
<ASPATH-LIST-NAME>	Specifies the name of the AS path list to match the AS path attribute of the route.

Example

Configuring a match clause in the route map to match the AS path list:

```
switch(config)# ip aspath-list ASLst permit 1001
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match aspath-list ASLst
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match community-list

```
match community-list <COMMUNITY-LIST-NAME> [exact-match]
no match community-list <COMMUNITY-LIST-NAME> [exact-match]
```

Description

Matches the community number attribute of the route with one, or more regular expressions in the community-list.

The **no** form of this command restores the default behavior of not matching the community number attribute of the route.

Parameter	Description
<code><COMMUNITY-LIST-NAME></code>	Specifies the name of the community-list to match the community number attribute of the route.
<code>[exact-match]</code>	Indicates that the community number attribute must match exactly with the expressions in the community-list. However, the order of the communities in the community-list is of no significance.

Example

Configuring a match clause in the route map to match the community list:

```
switch(config)# ip community-list standard CommLst 101:41 permit 12:201
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match community-list CommLst
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match interface

```
match interface <INTERFACE-NAME>
no match interface <INTERFACE-NAME>
```

Description

Matches the outgoing interface value of the route with the value configured in the match clause. This command is applicable to static and connected routes which will be redistributed to the BGP protocol. The **no** form of this command restores the default behavior of not matching the outgoing interface value of the route.

Parameter	Description
<code><INTERFACE-NAME></code>	Specifies the value to be matched with the outgoing interface of the route entry.

Example

Configuring a match clause in the route map to match the outgoing interface of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match interface 1/1/1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match ip address prefix-list

```
match ip address prefix-list <PREFIX-LIST-NAME>
no match ip address prefix-list <PREFIX-LIST-NAME>
```

Description

Matches the destination IP address prefix of the routes with one or more addresses in the prefix list.

The **no** form of this command restores the default behavior of not matching the destination IP address prefix of the routes to their default value. This command is applicable to OSPF, static, and connected routes which will be redistributed to the BGP protocol.

Parameter	Description
<PREFIX-LIST-NAME>	Specifies the name of the prefix list to be matched with the network address of the route.

Example

Configuring a prefix list and a match clause in route map to match the prefix list:

```
switch(config)# ip prefix-list PfxLst permit 4.0.0.0/8
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match ip address prefix-list PfxLst
```



When the IP prefix list with prefix and mask-length of 0.0.0.0/0 is used, the route matches default-route 0.0.0.0/0 as well as any other route. This behavior would be changed to match only the default-route in the next release.



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match ip next-hop

```
match {ip | ipv6} next-hop {<ADDRESS> | prefix-list <PREFIX-LIST-NAME>}
no match {ip | ipv6} next-hop [<ADDRESS> | prefix-list <PREFIX-LIST-NAME>]
```

Description

Matches the next-hop address of the route with the configured address in the match clause. This command is applicable to static routes which will be redistributed to BGP protocol.

The **no** form of this command restores the default behavior of not matching the next-hop address of the route.

Parameter	Description
<ADDRESS>	Specifies the IPv4 address to match with the next-hop address of the route.
prefix-list <PREFIX-LIST-NAME>	Specifies the name of the IP prefix list to be matched with the next-hop address of the route.

Example

Configuring a match clause in the route map to match the next-hop address of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match ip next-hop 1.1.1.2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match ip route-source

```
match ip route-source prefix-list <PREFIX-LIST-NAME>
no match ip route-source prefix-list <PREFIX-LIST-NAME>
```

Description

Matches the IP address of the source of the route using IP prefix lists.

The **no** form of this command restores the default behavior of not matching the IP address of the route.

Parameter	Description
<PREFIX-LIST-NAME>	Specifies the name of the prefix list to match the IP address of the source of the route.

Example

Configuring a match clause in the route map to match the source of the route:

```
switch(config)# ip prefix-list RouterLst 4.4.4.4/32
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match ip route-source prefix-list RouterLst
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match local-preference

```
match local-preference <VALUE>
no match local-preference <VALUE>
```

Description

Matches the local preference value of the route with the value configured in the match clause.

The **no** form of this command restores the default behavior of not matching the local preference value of the route.

Parameter	Description
<VALUE>	Specifies the value to be matched with the route entry local preference in the range of 1 to 4294967295.

Example

Configuring a match clause in the route map to match the local preference of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match local-preference 100
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match metric

```
match metric <VALUE>
no match metric <VALUE>
```

Description

Matches the MED value of the route with the value configured in the match clause.

The **no** form of this command restores the default behavior of not matching the MED value of the route.

Parameter	Description
<VALUE>	Specifies the value to be matched with the route entry MED.

Example

Configuring a match clause in the route map to match the metric of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match metric 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match origin

```
match origin {igp | egp | incomplete}
no match origin [igp | egp | incomplete]
```

Description

Matches the route origin attribute of the route with route configured in the match clause.

The **no** form of this command restores the default behavior of not matching the route origin attribute of the route.

Parameter	Description
{igp egp incomplete}	Specifies if the route origin attribute is matched with a match clause which originated as IGP, EGP, or has unknown origin. The unknown origin is typically redistributed from another routing protocol.

Example

Configuring a match clause in the route map to match the origin:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match origin igp
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match route-type

```
match route-type external {type-1 | type-2}
no match route-type external [type-1 | type-2]
```

Description

Matches the metric-type value of the OSPF external route with the value configured in the match clause. The **no** form of this command restores the default behavior of not matching the metric-type value of the OSPF external route.

Parameter	Description
{type-1 type-2}	Specifies the <i>type-1</i> or <i>type-2</i> OSPF value to be matched with the external route.

Example

Configuring a match clause in the route map to match the metric-type value of the OSPF external route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# match route-type external type-1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match source-protocol

```
match source-protocol {bgp | connected | ospf | static}
no match source-protocol [bgp | connected | ospf | static]
```

Description

Matches the source routing protocol value of the route with the value configured in the match clause. The **no** form of this command restores the default behavior of not matching the source routing protocol value of the route.

Parameter	Description
{bgp connected ospf static}	Specifies the <i>bgp</i> , <i>connected</i> , <i>ospf</i> , or <i>static</i> value to be matched with the route entry source protocol.

Example

Configuring a match clause in the route map to match the source protocol route:

```
switch(config)# route-map GlobalMap permit seq 11  
switch(config-route-map-GlobalMap-11)# match source-protocol ospf
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match tag

```
match tag <value>  
no match tag <value>
```

Description

Matches the tag value of the route with the one configured in the match clause. Applies to static routes that will be redistributed to BGP, OSPFv3 and OSPFv3 protocols.

The **no** form of this command removes the tag value of the route.

Parameter	Description
value	Numeric value to match with the route tag. Required.

Example

Configuring a match clause in route-map to match the tag value of the route:

```
switch(config)# route-map GlobalMap permit 11  
switch(config-route-map)# match tag 20
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

match vni

```
match vni <value>
no match vni <value>
```

Description

Matches the VNI value of the route with the one configured in the `match` clause. Applies to matching L2VNIs or L3VNIs. Use the `continue` clause if both L2VNI and L3VNI are to be matched. Route maps with the `match vni` clause can be used with L2VPN EVPN neighbors only.

The **no** form of this command removes the match for the VNI value of the route.

Parameter	Description
<code><value></code>	Numeric value to match with the route tag. Required. Range: 1 to 16777214

Example

Configuring a match clause in route map to match the VNI value of the route:

```
switch(config)# route-map GlobalMap permit 11
switch(config-route-map)# match vni 10000
```

Configuring a match clause in route map to match both L2VNI and L3VNI in a single route map:

```
switch(config)# route-map GlobalMap permit 11
switch(config-route-map)# match vni 10000
switch(config-route-map)# continue 12
switch(config)# route-map GlobalMap permit 12
switch(config-route-map)# match vni 10
```

The following example is different from the one above, as it configures a match clause in route map to match any one of the two VNIs:

```
switch(config)# route-map GlobalMap permit 10
switch(config-route-map)# match vni 10000
switch(config)# route-map GlobalMap permit 20
switch(config-route-map)# match vni 10
switch(config)# route-map GlobalMap deny 30
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

Set commands

set as-path exclude

```
set as-path exclude <AS>
no set as-path exclude <AS>
```

Description

Removes all occurrences of the configured AS Path from the AS Path attribute of the route. The **no** form of this command restores the default behavior of not modifying the AS Path attribute list.

Parameter	Description
<AS>	Specifies the AS number to be removed from the AS Path attribute of the route.

Example

Configuring a set clause in the route map to remove the AS from the AS Path attribute of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# set as-path exclude 1001
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set as-path prepend

```
set as-path prepend <AS> <AS>...  
no set as-path prepend <AS> <AS>...
```

Description

Pretends the list of the configured AS numbers to the AS Path attribute of the routes. To ensure that the AS path conforms to standards, the local AS is prepended after this command is executed.

The **no** form of this command restores the default behavior of not modifying the AS Path attribute list.

Parameter	Description
<AS> <AS>...	Specifies the AS numbers to be prepended from the AS Path attribute of the route.

Example

Configuring a set clause in the route map to prepend the AS from the AS Path attribute of the route:

```
switch(config)# route-map GlobalMap permit seq 11  
switch(config-route-map-GlobalMap-11)# set as-path prepend 1  
switch(config-route-map-GlobalMap-11)# no set as-path prepend 102
```



The **no** form of the command deletes the entire list of AS-Path prepend configuration regardless of the parameter list. In this example, the **no** form command would result in deletion of all the three AS numbers that were earlier configured.



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set community

```
set community {<AA:NN> | internet | no-export | no-advertise | local-as} [additive | delete]  
no set community [<AA:NN> | internet | no-export | no-advertise | local-as] [additive | delete]
```

Description

Modifies the community number attribute of the route with the value configured in the set clause. This command is applicable to OSPF, static, and connected routes which will be redistributed to the BGP protocol.

The **no** form of this command restores the default behavior of not modifying the community number attribute of the route.

Parameter	Description
{<AA:NN> internet no-export no-advertise local-as}	Selects the value to be set as the community number attribute of the route in the AA:NN format (quotation marks required when multiple communities are listed, for example: set community "65001:100 65001:200") or as a known community name internet , no-export , no-advertise , and local-as .
[additive]	Specifies that the specified community number is added to the existing community number attribute of the route.
[delete]	Specifies that the specified community number is removed from the existing community number attribute of the route.

Example

Configuring a set clause in the route map to modify the community number attribute of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# no set community 11:101
switch(config-route-map-GlobalMap-11)# set community no-advertise
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set dampening

```
set dampening {half-life <VALUE> reuse <VALUE> suppress <VALUE> max-suppress-time <VALUE>}
no set dampening
```

Description

Sets parameters of route flap dampening feature.

Parameter	Description
half-life	Time to reduce the penalty to half.
reuse	Lower threshold of penalty.
suppress	Upper threshold of penalty.
max-suppress-time	Max time to keep route suppressed.

Example

```
switch(config-route-map-abc-20)# set dampening half-life 5 reuse 50 suppress 125
max-suppress-time 255

switch(config-route-map-abc-20)# no set dampening half-life 5 reuse 50 suppress
125 max-suppress-time 255

switch(config-route-map-abc-20)# set dampening

switch(config-route-map-abc-20)# no set dampening
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set ip nexthop

```
set {ip | ipv6} nexthop {global} <IP-ADDR>
no set {ip | ipv6} nexthop {global} <IP-ADDR>
```

Description

Sets the IP address of the next-hop of the route with the value configured in the set clause.

The **no** form of this command restores the default behavior of not modifying the IP address of the next-hop of the route.



When a next-hop is changed via a route-map using the **set ip next-hop** command, the router-mac of the route remains unchanged. The router-mac of the route is changed/retained based on the **next-hop-self** and **next-hop-unchanged** configurations *only* if the next-hop is not changed via a route-map.

Parameter	Description
<code><IP-ADDR></code>	Specifies the IPv4 address to be set as the next-hop address of the route.

Example

Configuring a set clause in the route map to modify the next-hop address of the route entry:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# set ip nexthop 1.1.1.2
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set local-preference

```
set local-preference <VALUE>
no set local-preference <VALUE>
```

Description

Modifies the local-preference attribute of the route entry with the value configured in the set clause. The **no** form of this command restores the default behavior of not modifying the local-preference attribute of the route entry.

Parameter	Description
<code><VALUE></code>	Specifies the value to be set as the local-preference attribute of the route entry. Range: 0 to 4294967295.

Example

Configuring a set clause in the route map to modify the metric value of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# set local-preference 100
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set metric

```
set metric <VALUE>
no set metric <VALUE>
```

Description

Modifies the metric value of the route with the value configured in the set clause. This command is applicable to OSPF, static, and connected routes which will be redistributed to the BGP protocol. The **no** form of this command restores the default behavior of not modifying the metric value of the route.

Parameter	Description
<VALUE>	Specifies the value to be set as the metric value of the route. Range: 0 to 4294967295.

Example

Configuring a set clause in the route map to modify the metric value of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# set metric 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set origin

```
set origin [igp | egp | incomplete]
no set origin [igp | egp | incomplete]
```

Description

Modifies the route origin attribute of the route update with the value configured in the set clause.

The **no** form of this command restores the default behavior of not modifying the route origin attribute of the route.

Parameter	Description
{igp egp incomplete}	Selects the route update originated to IGP, EGP, or incomplete. When incomplete is selected, the route update origin is set to unknown.

Example

Configuring a set clause in the route map to modify the origin attribute of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap-11)# set origin igp
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set tag

```
set tag <value>
[no] set tag <value>
```

Description

Modifies the tag value of the route with the one configured in the set clause. Applicable to static routes that will be redistributed to ospfv2 and ospfv3 protocols.

The **no** form of this command removes the set clause tag value.

Parameter	Description
value	Numeric value to change the route entry tag. Range: 0-4294967295. Required.

Example

Configuring a set clause in route-map to modify the tag value of the route:

```
switch(config)# route-map GlobalMap permit 11
switch(config-route-map)# set tag 10
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

set weight

```
set weight <VALUE>
no set weight <VALUE>
```

Description

Modifies the weight attribute of the route with the value configured in the set clause.

The **no** form of this command restores the default behavior of not modifying the weight attribute of the route.

Parameter	Description
<VALUE>	Specifies the value to be set as the weight attribute of the route. Range: 0 to 65535.

Example

Configuring a set clause in the route map to modify the metric value of the route:

```
switch(config)# route-map GlobalMap permit seq 11
switch(config-route-map-GlobalMap=11)# set weight 100
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config-route-map	Administrators or local user group members with execution rights for this command.

Show commands

show ip aspath-list

```
show ip aspath-list [<NAME>] [vsx-peer]
```

Description

Shows the configuration details of the AS path list.

Parameter	Description
<NAME>	Specifies name of the AS path list.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IP AS path list configuration information:

```
switch# show ip aspath-list
ip aspath-list ASLst
  seq 10 permit 22 33
  seq 20 deny 44
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show ip community-list

show ip community-list [<NAME>] [vsx-peer]

Description

Shows the configuration details of the community-list.

Parameter	Description
<NAME>	Specifies name of the community-list.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the community list configuration information:

```
switch# show ip community-list
ip community-list standard CommLst
  seq 10 permit 11:101
  seq 20 deny 12:201
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show ip prefix-list

show ip prefix-list [<NAME>] [vsx-peer]

Description

Shows the configuration details of the IP prefix lists.

Parameter	Description
<NAME>	Specifies name of the IP prefix lists.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IP prefix list configuration information:

```
switch# show ip prefix-list
ip prefix-list PfxLst: 2 entries
  seq 10 permit 3.0.0.0/8 ge 8 le 8
  seq 20 deny 4.0.0.0/8 ge 8 le 8
```

```
switch# show ipv6 prefix-list
ipv6 prefix-list x: 1 entries
      seq      10 permit 2011::/64ge 64le 64
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

show route-map

show route-map [<NAME>] [vsx-peer]

Description

Shows the configuration details of the route map.

Parameter	Description
<NAME>	Specifies name of the route map.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the route map configuration information:

```
switch# show route-map
Route map: InternetFilter
  Seq 10, permit,
    Match :
      origin : egp
      metric : 123
    Set :
      community : 23:34
      metric : 3
      as_path_exclude : 123
      local_preference : 3456
      origin : igp
      weight : 25
  Seq 20, permit,
    Match :
      origin : egp
      metric : 456
    Set :
      community : 44:44
      metric : 5
      as_path_prepend : 444
      local_preference : 66
      origin : igp
      weight : 250

Route map: LocalFilter
  Seq 10, permit,
    origin : egp
    metric : 10

    local-preference          : 20
    route-type                : external_type1
    source-protocol           : static
    prefix-list               : PfxLst
    aspath-list               : ASLst
    community-list            : CommLst
    ip next-hop prefix-list    : PfxLst
    ip route-source prefix-list : PfxLst
  Set :
    community : 22:33
    metric : 25
    as_path prepend : 65535 65534

    local_preference : 30
    origin : igp
    weight : 30
```

ip next-hop address : 2.2.2.3

ip next-hop address : 2.2.2.4

```
dampening : half-life = 5, reuse = 50, suppress = 125,  
max-suppress-time = 15
```

All the match clauses are grouped. All the set clauses are grouped.



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	Manager (#)	Administrators or local user group members with execution rights for this command.

clear spanning-tree statistics

`clear spanning-tree statistics [VLAN-ID]`

Description

Clears the spanning tree BPDU statistics, either all statistics or those related to a specified VLAN.

Parameter	Description
VLAN-ID	Specifies the VLAN ID.

Example

Clearing all spanning tree BPDU statistics:

```
switch(config)# clear spanning-tree statistics
```

Clearing spanning tree BPDU statistics for a particular VLAN :

```
switch(config)# clear spanning-tree statistics 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

show capacities-status rpvst

`show capacities-status rpvst`

Description

Shows the number of RPVST VLANs and RPVST VPORTs currently configured.

Examples

Showing capacities-status:

```
switch# show capacities-status rpvst
System Capacities Status : Filter RPVST
Capacities Status Name      Value      Maximum
-----
Number of RPVST VLANs configured    3          254
Number of RPVST VPORTs configured   9         2048
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree

```
show spanning-tree [vsx-peer]
```

Description

Shows the spanning tree mode and information on the RPVST instances.

When Port security is enabled on the port and the client is not-yet authenticated, the security feature keeps the port in the **Down** state. STP also keeps the port in the **Blocking** state and the role as **Disabled** in the **show spanning-tree** command output, whereas in the hardware, the state is maintained as **Learning**. After client authentication is successful, the port state changes to **Forwarding**.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing spanning tree mode and RPVST instance information:

```
switch# show spanning-tree
Spanning tree status      : Enabled Protocol: RPVST
Extended System-id       : Enabled
Ignore PVID Inconsistency : Enabled
Path cost method          : Long
RPVST-MSTP Interconnect VLAN : 1
Current Virtual Ports Count : 7
Maximum Allowed Virtual Ports : 2048

VLAN1
  Root ID    Priority    : 32768
             MAC-Address: 70:72:cf:31:c9:23
             This bridge is the root
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

  Bridge ID  Priority    : 32768
             MAC-Address: 70:72:cf:31:c9:23
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

PORT      ROLE        STATE        COST      PRIORITY  TYPE        BPDU-Tx  BPDU-Rx  TCN-Tx  TCN-Rx
-----
1/1/1     Designated Forwarding  20000     128       P2P Edge    100       60       20       10
1/1/2     Designated Forwarding  20000     128       P2P         100       60       20       10
1/1/3     Designated Forwarding  20000     128       Shr         100       60       20       10
1/1/4     Designated Forwarding  20000     128       Shr Edge    100       60       20       10
1/1/5     Alternate Loop-Inc    20000     128       Shr Edge    100       60       20       10
1/1/6     Alternate Root-Inc    20000     128       Shr Edge    100       60       20       10
1/1/7     Disabled   Down         20000     128       P2P         100       60       20       10

Number of topology changes      : 4
Last topology change occurred  : 516 seconds ago
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state <code>Down</code> is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree detail

```
show spanning-tree detail [vsx-peer]
```

Description

Shows the detailed spanning tree mode and information on the RPVST instances.

When Port security is enabled on the port and the client is not-yet authenticated, the security feature keeps the port in the **Down** state. STP also keeps the port in the **Blocking** state and the role as **Disabled** in the **show spanning-tree** command output, whereas in the hardware, the state is maintained as **Learning**. After client authentication is successful, the port state changes to **Forwarding**.

Parameter	Description
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing spanning tree mode and detailed RPVST instance information:

```
switch# show spanning-tree detail
Spanning tree status      : Enabled Protocol: RPVST AUTO
Extended System-id       : Enabled
Ignore PVID Inconsistency : Disabled
Path cost method          : Long
RPVST-MSTP Interconnect VLAN : 1
Current Virtual Ports Count : 2032
Maximum Allowed Virtual Ports : 2048
Maximum Allowed RPVST Instances: 254
Configured RPVST Enable Vlans : 20-30,100
Configured RPVST Disable Vlans : 1-10
Auto RPVST Enable Vlans      : 11-19,31-99,101-264
Vlans with no RPVST Instance due to Max limit reach : 265-300

VLAN1
  Root ID    Priority    : 32768
             MAC-Address: 70:72:cf:31:c9:23
             This bridge is the root
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

  Bridge ID  Priority    : 32768
             MAC-Address: 70:72:cf:31:c9:23
             Hello time(in seconds):2  Max Age(in seconds):20
             Forward Delay(in seconds):15

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx  TCN-Tx  TCN-Rx
-----
1/1/1     Designated Forwarding 20000     128       P2P Edge  100       60       20       10
1/1/2     Designated Forwarding 20000     128       P2P      100       60       20       10
1/1/3     Designated Forwarding 20000     128       Shr      100       60       20       10
1/1/4     Designated Forwarding 20000     128       Shr Edge  100       60       20       10
1/1/5     Alternate  Loop-Inc  20000     128       Shr Edge  100       60       20       10
1/1/6     Alternate  Root-Inc  20000     128       Shr Edge  100       60       20       10
1/1/7     Disabled   Down      20000     128       P2P      100       60       20       10
lag1      Disabled   Down      20000     128       P2P Bound 100       60       20       10
```

```

Topology change flag : False
Number of topology changes : 1
Last topology change occurred : 33293 seconds ago

Port 1/1/1
Designated Root Priority      : 32768      Address: 48:0F:CF:AF:22:1D
Designated Bridge Priority    : 32768      Address: 48:0F:CF:AF:22:1D
Designated Port              : 1/1/1
Forwarding-State transitions  : 0
BPDUs sent 1582, received 1506
TCN_Tx: 10, TCN_Rx: 10

Port lag1
Designated Root Priority      : 32768      Address: 48:0F:CF:AF:22:1D
Designated Bridge Priority    : 32768      Address: 48:0F:CF:AF:22:1D
Designated Port              : lag1
Forwarding-State transitions  : 0
BPDUs sent 1402, received 1316
TCN_Tx: 10, TCN_Rx: 10
Multi-chassis role           : active

```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree inconsistent-ports

show spanning-tree inconsistent-ports [vlan <VLAN-ID>]

Description

Shows ports blocked by STP protection functions such as Root guard, Loop guard, BPDU guard, and RPVST guard.

Parameter	Description
<VLAN-ID>	Specifies a VLAN ID number.

Examples

Showing inconsistent port information:

```
switch# show spanning-tree inconsistent-ports
VLAN ID      Blocked Port      Reason
-----
1             1/1/1             BPDU Guard
2             1/1/1             BPDU Guard
3             1/1/1             BPDU Guard
4             1/1/1             BPDU Guard
5             1/1/1             BPDU Guard
6             1/1/1             BPDU Guard
7             1/1/1             BPDU Guard
8             1/1/1             BPDU Guard
9             1/1/1             BPDU Guard
10            1/1/1             BPDU Guard
```

Showing inconsistent port information for VLANs 1 to 4:

```
switch# show spanning-tree inconsistent-ports vlan 1-4
VLAN ID      Blocked Port      Reason
-----
1             1/1/3             Root Guard
2             1/1/7             BPDU Guard
3             1/1/9             Loop Guard
4             1/1/37            RPVST Guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree summary port

```
show spanning-tree summary port
```

Description

Shows a summary of port-related spanning-tree configuration and status.

Example

Showing a summary of port-related spanning tree information:


```
switch# show spanning-tree summary port

STP status           : Enabled
Protocol             : RPVST
BPDU guard timeout value : None
BPDU guard enabled interfaces : 1/1/1
BPDU filter enabled interfaces : None
Root guard enabled interfaces : 1/1/3
Loop guard enabled interfaces : 1/1/2
TCN guard enabled interfaces : 1/1/1-1/1/3
```

Interface count by state

VLAN	Blocking	Listening	Learning	Forwarding	Down
VLAN1	0	0	0	1	0
VLAN2	0	0	0	1	0
Total = 2	0	0	0	2	0



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree summary root

```
show spanning-tree summary root
```

Description

Shows the summary of spanning tree root and configurations for all VLANs.

Example

Showing summary of spanning tree configurations:

```
switch# show spanning-tree summary root

STP status           : Enabled
```

```
Protocol          : RPVST
System ID         : f8:60:f0:c9:70:40
```

```
Root bridge for VLANs : 1-10
```

VLAN	Priority	Root ID	Root cost	Hello Time	Max Age	Fwd Dly	Root Port
VLAN1	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN2	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN3	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN4	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN5	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN6	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN7	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN8	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN9	32768	f8:60:f0:c9:70:40	0	2	20	15	0
VLAN10	32768	f8:60:f0:c9:70:40	0	2	20	15	0



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree vlan

```
show spanning-tree vlan <VLAN-ID> [vsx-peer]
```

Description

Displays the spanning tree mode and information on the RPVST instance of the specified VLAN.

Parameter	Description
<VLAN-ID>	Specifies the number of a VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing spanning tree mode and RPVST instance information for VLAN 2:

```
switch# show spanning-tree vlan 2
VLAN2
Spanning tree status: Enabled Protocol: RPVST
  Root ID      Priority    : 32768
                MAC-Address: 70:72:cf:76:43:2a
                This bridge is the root
                Hello time(in seconds):2   Max Age(in seconds):20
                Forward Delay(in seconds):15

  Bridge ID    Priority    : 32768
                MAC-Address: 70:72:cf:76:43:2a
                Hello time(in seconds):2   Max Age(in seconds):20
                Forward Delay(in seconds):15

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx
TCN-Tx    TCN-Rx
-----
1/1/1     Designated Forwarding 20000     128       P2P Edge  100       60
20        10
1/1/2     Designated Forwarding 20000     128       P2P      100       60
20        10
1/1/3     Designated Forwarding 20000     128       Shr      100       60
20        10
1/1/4     Designated Forwarding 20000     128       Shr Edge  100       60
20        10
1/1/5     Alternate Loop-Inc  20000     128       Shr Edge  100       60
20        10
1/1/6     Alternate Root-Inc  20000     128       Shr Edge  100       60
20        10
1/1/7     Disabled   Down      20000     128       P2P      100       60
20        10

Number of topology changes : 4
Last topology change occurred : 516 seconds ago
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show spanning-tree vlan detail

show spanning-tree vlan <VLAN-ID> detail [vsx-peer]

Description

Displays the spanning tree mode and information on the RPVST instance of the specified VLAN and optionally displays details on the RPVST instance for the VLAN.

Parameter	Description
<VLAN-ID>	Specifies the number of a VLAN.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing spanning tree mode and detailed RPVST instance information for VLAN 2:

```
switch# show spanning-tree vlan 2 detail
VLAN2
Spanning tree status: Enabled Protocol: RPVST
  Root ID      Priority    : 32768
                MAC-Address: 70:72:cf:76:43:2a
                This bridge is the root
                Hello time(in seconds):2   Max Age(in seconds):20
                Forward Delay(in seconds):15

  Bridge ID    Priority    : 32768
                MAC-Address: 70:72:cf:76:43:2a
                Hello time(in seconds):2   Max Age(in seconds):20
                Forward Delay(in seconds):15

PORT      ROLE      STATE      COST      PRIORITY  TYPE      BPDU-Tx  BPDU-Rx
TCN-Tx    TCN-Rx
-----
1/1/1     Designated Forwarding 20000     128       P2P Edge  100       60
20        10
1/1/2     Designated Forwarding 20000     128       P2P      100       60
20        10
1/1/3     Designated Forwarding 20000     128       Shr      100       60
20        10
1/1/4     Designated Forwarding 20000     128       Shr Edge  100       60
20        10
1/1/5     Alternate Loop-Inc  20000     128       Shr Edge  100       60
20        10
1/1/6     Alternate Root-Inc  20000     128       Shr Edge  100       60
20        10
1/1/7     Disabled   Down       20000     128       P2P      100       60
20        10

Topology change flag : False
Number of topology changes : 1
Last topology change occurred : 33293 seconds ago

Port 1/1/1
```

```
Designated root has priority :32768 Address: 48:0f:cf:af:22:1d
Designated bridge has priority :32768 Address: 48:0f:cf:af:22:1d
Designated port :1
Number of transitions to forwarding state : 0
BPDUs sent 1582, received 1506
TCN_Tx: 10, TCN_Rx: 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.09	A new state Down is added in the output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

spanning-tree bpdu-guard timeout

```
spanning-tree bpdu-guard timeout <INTERVAL>
no spanning-tree bpdu-guard timeout [<INTERVAL>]
```

Description

Enables and configures the auto re-enable timeout in seconds for all interfaces with BPDU guard enabled. When an interface is disabled after receiving an unauthorized BPDU it will automatically be re-enabled after the timeout expires. The default is for the interface to stay disabled until manually re-enabled.

The **no** form of the command disables BPDU guard timeout. This is the default.

Parameter	Description
<INTERVAL>	Specifies the re-enable timeout in seconds. Range: 1 to 65535.

Example

Enabling the BPDU guard timeout:

```
switch(config) # spanning-tree bpdu-guard timeout 10
```

Disabling BPDU guard timeout:

```
switch(config)# no spanning-tree bpduguard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree extend-system-id

```
spanning-tree extend-system-id {enable | disable}  
no spanning-tree extend-system-id
```

Description

Configures use of extended system ID. When enabled, the VLAN ID is included in spanning tree packets. When disabled, the VLAN ID is set to NULL in the spanning tree packets.

By default, extended system ID is enabled. If you disable extended system ID, the bridge identifier field in the spanning tree packet is filled with zeros.

The **no** form of this command disables extended system ID.

Parameter	Description
enable	Specifies enabling use of extended system ID.
disable	Specifies disabling use of extended system ID.

Examples

Enabling extended system ID:

```
switch# config  
switch(config)# spanning-tree extend-system-id enable
```

Disabling extended system ID:

```
switch# config
switch(config)# spanning-tree extend-system-id disable
switch(config)# no spanning-tree extend-system-id
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree ignore-pvid-inconsistency

```
spanning-tree ignore-pvid-inconsistency {enable | disable}
no spanning-tree ignore-pvid-inconsistency
```

Description

Configures port behavior when per-VLAN ID inconsistencies are present. For example, when the ports on both ends of a point-to-point link are untagged members of different VLANs, enabling this option allows RPVST+ to process untagged RPVST+ packets belonging to the peer's untagged VLAN as if they were received on the current device's untagged VLAN. When this option is disabled, RPVST+ blocks the link, causing traffic on the mismatched VLANs to be dropped.

If this option is enabled on multiple switches connected by hubs, there could be more than two VLANs involved in PVID mismatches that will be ignored by RPVST+.

If port VLAN memberships is misconfigured on a switch in the network, then enabling this option prevents RPVST+ from detecting the problem, which may result in packet duplication in the network since RPVST+ would not converge correctly.

This command affects all ports on the switch belonging to VLANs on which RPVST+ is enabled.

By default ignore per-VLAN ID inconsistency is disabled.

The **no** form of this command sets the ignore per-VLAN ID inconsistencies to disabled.

Parameter	Description
enable	Specifies ignore per-VLAN ID inconsistencies and allow RPVST to run on mismatched links.
disable	Disables the ignore per-VLAN ID inconsistencies functionality.

Examples

Enabling ignore per-VLAN ID inconsistencies:

```
switch# config
switch(config)# spanning-tree ignore-pvid-inconsistency enable
```

Disabling ignore per-VLAN ID inconsistencies:

```
switch# config
switch(config)# spanning-tree ignore-pvid-inconsistency disable
switch(config)# no spanning-tree ignore-pvid-inconsistency
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree link-type

```
spanning-tree link-type {point-to-point | shared}
no spanning-tree link-type
```

Description

Configures the link type of a port.

The **no** form of this command sets the spanning tree link type to the default value of **point-to-point**.

Parameter	Description
point-to-point	Sets the spanning tree link type as point-to-point. Use this for full-duplex ports that provide a point-to-point link to devices such as a switch, bridge, or end-node. Default.
shared	Sets the spanning tree link type as shared. Use this when the port is connected to a hub.

Examples

Setting spanning tree link type to shared:


```
switch(config)# interface 1/1/1  
switch(config-if)# spanning-tree link-type shared
```

Setting spanning tree link type to point-to-point for a port:

```
switch(config)# interface 1/1/1  
switch(config-if)# no spanning-tree link-type
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree mode

```
spanning-tree mode {mstp|rpvst [auto-vlan-enable [priority <NUMBER>]]}  
no spanning-tree mode {mstp|rpvst [auto-vlan-enable [priority <NUMBER>]]}
```

Description

Sets the spanning tree protocol (STP) mode to either MSTP mode (Multiple-instance Spanning Tree Protocol) or RPVST mode (Rapid Per VLAN Spanning Tree). Enabling the RPVST Auto VLAN feature will run RPVST on all VLANs currently configured on the switch. Default priority of 8 will be assigned to the VLANs being auto created.

The **no** form of this command sets the spanning tree mode to the default **mstp**.



Enabling auto-VLAN can lead to an undeterministic state if auto scaled beyond the max system limit mentioned in the capacity-status.

Parameter	Description
mstp	Sets the STP mode to MSTP which applies spanning tree separately for each set of VLANs called an MSTI (multiple spanning tree instance).

Parameter	Description
<code>rpvst</code>	Sets the STP mode to RPVST.
<code>auto-vlan-enable</code>	Selects RPVST auto VLAN mode.
<code>priority <NUMBER></code>	Specifies the priorities for all auto created RPVST instances. Configured as a multiple of 4096. Default: 8.

Examples

Enabling MSTP mode:

```
switch(config) # spanning-tree mode mstp
```

Disabling MSTP mode:

```
switch(config) # no spanning-tree mode mstp
```

Enabling RPVST mode:

```
switch(config) # spanning-tree mode rpvst
```

Disabling RPVST mode:

```
switch(config) # no spanning-tree mode rpvst
```

Enabling RPVST auto VLAN with a priority of 1:

```
switch(config) # spanning-tree mode rpvst auto-vlan-enable priority 1
```

Disabling RPVST auto VLAN with a priority of 1:

```
switch(config) # no spanning-tree mode rpvst auto-vlan-enable priority 1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.12.1000	Auto VLAN enable added.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree pathcost-type

```
spanning-tree pathcost-type {long | short}
no spanning-tree pathcost-type [long|short]
```

Description

Configures the spanning tree path cost type. The long mode provides support for the wider range of link speeds required by high-speed interfaces. All switches in the network must use the same path cost type or errors can occur in the spanning tree.

The **no** form of this command sets the spanning tree path cost type to the default **long**.

Parameter	Description
long	Specifies the spanning tree path cost type as a 32-bit value, allowing port cost values to be set in the range 1-200,000,000. Default.
short	Specifies the spanning tree path cost type as a 16-bit value, allowing port cost values to be set in the range 1-65535.

Examples

Setting spanning tree path cost type to short:

```
switch# config
switch(config)# spanning-tree pathcost-type short
```

Setting spanning tree path cost type to long:

```
switch# config
switch(config)# spanning-tree pathcost-type long
```

Setting spanning tree path cost to default of long:

```
switch# config
switch(config)# no spanning-tree pathcost-type
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree rpvst-mstp interconnect vlan

```
spanning-tree rpvst-mstp-interconnect-vlan <VLAN-ID>
no spanning-tree rpvst-mstp-interconnect-vlan [<VLAN-ID>]
```

Description

Configures the VLAN that has to be used to interconnect RPVST and MSTP domains. VLAN 1 is used by default.

The **no** form of this command sets the VLAN configuration to the default of 1.

- It is required to create the interconnect VLAN and then configure RPVST spanning tree on it.
- The same interconnect VLAN must be kept on all the switches in the network.
- Adding or deleting the interconnect VLAN triggers a re-convergence in the network.
- Deleting a VLAN that is configured as the interconnect VLAN does not reset the value to the default.

Parameter	Description
<VLAN-ID>	Specifies the number of a VLAN.

Examples

This example configures VLAN 10 to used to interconnect RPVST and MSTP domains.

```
switch#(config)# spanning-tree rpvst-mstp-interconnect-vlan 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree tcn-guard

```
spanning-tree tcn-guard
no spanning-tree tcn-guard
```

Description

Disables propagation of topology change notifications (TCNs) to other STP ports. Use this when you do not want topology changes to be noticed by peer devices. By default, the propagation is enabled.

The **no** form of this command, enables propagation of topology changes which is the default.

Examples

Enabling `tcn-guard`, which disables propagation of topology changes:

```
switch(config-if) # spanning-tree tcn-guard
```

Disabling `tcn-guard`, which enables propagation of topology changes:

```
switch(config-if) # no spanning-tree tcn-guard
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree vlan

```
spanning-tree vlan <VLAN-LIST> [{hello-time | foward-delay | max-age | priority} <VALUE>]
no spanning-tree vlan <VLAN-LIST> [hello-time | foward-delay | max-age | priority]
```

Description

Creates an RPVST instance for the specified VLAN. This command also allows for configuration of RPVST instance-specific time parameters.

The **no** form of this command removes the RPVST instance associated with the specified VLAN, and configures default values for RPVST instance-specific parameters.

Parameter	Description
<VLAN-LIST>	Specifies the number of a single VLAN, or a series of numbers for a range of VLANs, separated by commas (1, 2, 3, 4), dashes (1-4), or both (1-4,6).
hello-time <VALUE>	Specifies the hello-time in seconds for the RPVST instance. Range: 2-10 seconds. Default: 2 seconds.
forward-delay <VALUE>	Specifies the forward-delay time in seconds for the RPVST instance. Range: 4-30 seconds. Default: 15 seconds.
max-age <VALUE>	Specifies the maximum age time in seconds for the RPVST instance. Range: 6-40 seconds. Default: 20 seconds.
priority <VALUE>	Specifies the priority for the RPVST instance. Priority value is configured as a multiple of 4096. Range: 0-15. Default: 8 which is 32768.

Examples

Creating an RPVST instance for a list of VLANs and configuring various time parameters:

```
switch# config
switch(config)# spanning-tree vlan 2-5
switch(config)# spanning-tree vlan 2-5 hello-time 5
switch(config)# spanning-tree vlan 5 max-age 10
switch(config)# spanning-tree vlan 2-5 forward-delay 25
switch(config)# spanning-tree vlan 2-5 priority 5
```

Removing an RPVST instance for a list of VLANs and setting various time parameters to the default:

```
switch# config
switch(config)# no spanning-tree vlan 2-5
switch(config)# no spanning-tree vlan 2-5 hello-time
switch(config)# no spanning-tree vlan 2-5 forward-time
switch(config)# no spanning-tree vlan 2-5 max-age
switch(config)# no spanning-tree vlan 2-5 priority
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

spanning-tree vlan cost

```
spanning-tree vlan <VLAN-LIST> cost <PORT-COST>
no spanning-tree vlan <VLAN-LIST> cost
```

Description

Configures the spanning tree cost for the VLAN. This is the cost to reach the root port. The **no** form of this command sets the port cost to the default value.

Parameter	Description
<VLAN-LIST>	Specifies the number of a single VLAN, or a series of numbers for a range of VLANs, separated by commas (1, 2, 3, 4), dashes (1-4), or both (1-4,6).
<PORT-COST>	Specifies the spanning tree cost for the VLAN. Range: 1-200,000,000. Default is calculated from the port link speed: 10 Mbps link speed equals a path cost of 2,000,000. 100 Mbps link speed equals a path cost of 200,000. 1 Gbps link speed equals a path cost of 20,000. 2 Gbps link speed equals a path cost of 10,000. 10 Gbps link speed equals a path cost of 2,000. 100 Gbps link speed equals a path cost of 200. 1 Tbps link speed equals a path cost of 20.

Examples

Setting port cost:

```
switch(config-if)# spanning-tree vlan 5 cost 100000
```

Setting port cost to the default:

```
switch(config-if)# no spanning-tree vlan 5 cost
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree vlan port-priority

```
spanning-tree vlan <VLAN-LIST> port-priority <PRIORITY>
no spanning-tree vlan <VLAN-LIST> port-priority
```

Description

Configures port priority. A port with the lowest priority number has the highest priority for use in forwarding traffic.

The **no** form of this command, sets the port priority to the default of 8.

Parameter	Description
<VLAN-LIST>	Specifies the number of a single VLAN, or a series of numbers for a range of VLANs, separated by commas (1, 2, 3, 4), dashes (1-4), or both (1-4,6).
<PRIORITY>	Specifies the port priority. The value, configured as a multiple of 16, helps in determining the designated port. The lower a priority value, the higher the priority. Range: 1 to15. Default: 8.

Examples

Setting port priority:

```
switch(config-if) # spanning-tree vlan 5 port-priority 10
```

Setting port priority to the default of 8:

```
switch(config-if) # no spanning-tree vlan 5 port-priority
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

spanning-tree trap

```
spanning-tree trap {new-root | topology-change [vlan <VLAN-ID>] |  
    errant-bpdu | root-guard-inconsistency | loop-guard-inconsistency}  
no spanning-tree trap {new-root | topology-change [vlan <VLAN-ID>] |  
    errant-bpdu | root-guard-inconsistency | loop-guard-inconsistency}
```

Description

Enables SNMP traps for new root, topology change event, errant-bpdu received event, root-guard inconsistency, and loop-guard inconsistency notifications. It is disabled by default.

The **no** form of this command disables the notifications for SNMP traps.

Parameter	Description
new-root	Enables SNMP notification when a new root is elected on any PVST vlan on the switch.
topology-change	Enables SNMP notification when a topology change event occurred in specified PVST vlan on the switch.
<VLAN-ID>	Specifies the VLAN ID for the topology change trap. Range: 1 to 4094.
errant-bpdu	Enables SNMP notification when an errant bpdu is received by any PVST vlan on the switch.
root-guard-inconsistency	Enables SNMP notification when the root-guard finds the port inconsistent for any PVST vlan on the switch.
loop-guard-inconsistency	Enables SNMP notification when the loop-guard finds the port inconsistent for any PVST vlan on the switch.

Examples

Enabling the notifications for the SNMP traps:

```
switch(config)# spanning-tree trap  
    new-root          Enable notifications which are sent when a new root is  
    elected  
    topology-change   Enable notifications which are sent when a topology  
change occurs  
    errant-bpdu       Enable notifications which are sent when an errant  
bpdu is received  
    root-guard-inconsistency Enable notifications which are sent when root guard  
inconsistency occurs  
    loop-guard-inconsistency Enable notifications which are sent when loop guard  
inconsistency occurs  
switch(config)# spanning-tree trap new-root  
<cr>  
switch(config)# spanning-tree trap topology-change  
    vlan Enable topology change notification for the specified PVST vlan id.  
switch(config)# spanning-tree trap topology-change vlan  
<1-4094> Enable topology change information on the specified vlan id.  
switch(config)# spanning-tree trap topology-change vlan 1  
<cr>  
switch(config)# spanning-tree trap errant-bpdu  
<cr>  
switch(config)# spanning-tree trap root-guard-inconsistency
```

```
<cr>
switch(config)# spanning-tree trap loop-guard-inconsistency
<cr>
```

Disabling the notifications for the SNMP traps:

```
switch(config)# no spanning-tree trap
    new-root          Disable notifications which are sent when a new root
is elected
    topology-change   Disable notifications which are sent when a topology
change occurs
    errant-bpdu       Disable notifications which are sent when an errant
bpdu is received
    root-guard-inconsistency Disable notifications which are sent when root guard
inconsistency occurs
    loop-guard-inconsistency Disable notifications which are sent when loop guard
inconsistency occurs
switch(config)# no spanning-tree trap new-root
<cr>
switch(config)# no spanning-tree trap topology-change
    instance Disable topology change notification for the specified PVST vlan id.
switch(config)# no spanning-tree trap topology-change vlan
    <1-4094> Disable topology change information on the specified PVST vlan id.
switch(config)# no spanning-tree trap topology-change vlan 1
<cr>
switch(config)# no spanning-tree trap errant-bpdu
<cr>
switch(config)# no spanning-tree trap root-guard-inconsistency
<cr>
switch(config)# no spanning-tree trap loop-guard-inconsistency
<cr>
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

fastboot

fastboot
no fastboot

Description

Enables fastboot for the system.

The **no** form of this command disables fastboot for the system.

Usage

When fastboot is enabled, most tests under a Power On Self Test (POST) are skipped. By default, fastboot is enabled.

After disabling fastboot, save switch configurations and then reboot for POST to run. POST verifies the hardware functionality of various modules during boot-up. Based on the criticality of the test, the selftest module decides whether to go ahead with the boot-up sequence of a particular subsystem or interface during a POST failure.

POST runs memory built-in selftest (BISTs) and front-end port loopback tests. Memory BISTs verify the internal and external memory blocks present in the module. The memory tables are critical for proper functionality of the system so any failures in these tests results in the corresponding subsystem to be marked as "Failed" and thus that subsystem is not available for use.

Front-end port loopback tests verify the physical port front-end interface. These tests check if a particular interface can function properly. A test failure means that a particular interface has been marked as "Failed" and is now unavailable for use.

Examples

Enabling fastboot:

```
switch# configure terminal
switch(config)# fastboot
switch(config)# end
switch# show running-config
Current configuration:
!
!Version AOS-CX ML.10.06.0001
module 1/1 product-number j1726a!Version AOS-CX FL.10.06.0001
module 1/1 product-number j1661a!Version AOS-CX XL.10.00.0002
module 1/1 product-number j1363a!Version AOS-CX PL.10.06.0001
module 1/1 product-number j1677a
!
!
!
!
!
```

```

!
vlan 1
interface 1/1/1
    no shutdown
    no routing

```

Disabling fastboot:

```

switch# configure terminal
switch(config)# no fastboot
switch(config)# end
switch(config)# write mem
Configuration changes will take time to process, please be patient.
switch# show running-config
Current configuration:
!
!Version AOS-CX ML.10.06.0001
module 1/1 product-number j1726a!Version AOS-CX FL.10.06.0001
module 1/1 product-number j1661a!Version AOS-CX XL.10.00.0002
module 1/1 product-number j1363a!Version AOS-CX PL.10.06.0001
module 1/1 product-number j1677a
!
!
!
no fastboot
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
    no routing

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show selftest

```

show selftest [brief] [vsx-peer]
show selftest line-module < SLOT-ID>
show selftest line-module < SLOT-ID> interface [brief] [vsx-peer]

```

```
show selftest interface [<PORT-NUM>] [vsx-peer]
```

Description

Displays selftest results.

Parameter	Description
[brief]	Shows the selftest results as a brief description. Default.
line-module	Shows the selftest results for a line module.
<SLOT-ID>	Shows the selftest results for the slot ID of the line or fabric module.
<PORT-NUM>	Shows the selftest results for the port number.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Displaying the output when fastboot is enabled:

```
switch# show selftest interface 1/1/2
Name      Status      ErrorCodes LastRunTime
-----
1/1/2     skipped      0x0

switch# show selftest line-module 1/1 interface
Name      Status      ErrorCodes LastRunTime
-----
1/1/1     skipped      0x0
1/1/2     skipped      0x0
1/1/3     skipped      0x0
1/1/31    skipped      0x0
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

clear sflow statistics

```
clear sflow statistics {global | interface <INTERFACE-NAME>}
```

Description

This command clears the sFlow sample statistics counter to 0 either globally or for a specific interface.

Parameter	Description
global	Specifies all interfaces on the switch.
interface <INTERFACE-NAME>	Specifies the name of an interface on the switch.

Examples

Clearing the global sFlow sample statistics counter to 0 globally:

```
switch(config)# clear sflow statistics global
```

Clearing the global sFlow sample statistics counter to 0 for interface 1/1/1:

```
switch(config)# clear sflow statistics interface 1/1/1
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow

sflow

```
no sflow
```

Description

Enables the sFlow agent.

- In the **config** context, this command enables the sFlow agent globally on all interfaces.
- In an **config-if** context, this command enables the sFlow agent on a specific interface. sFlow cannot be enabled on a member of a LAG, only on the LAG.

The sFlow agent is disabled by default.

The **no** form of this command disables the sFlow agent and deletes all sFlow configuration settings, either globally, or for a specific interface.

Examples

Enabling sFlow globally on all interfaces:

```
switch(config)# sflow
```

Disabling sFlow globally on all interfaces:

```
switch(config)# no sflow
```

Enabling sFlow on interface **1/1/1**:

```
switch(config)# interface 1/1/1  
switch(config-if)# sflow
```

Disabling sFlow on interface **1/1/1**:

```
switch(config)# interface 1/1/1  
switch(config-if)# no sflow
```

Enabling sFlow on interface **lag100**:

```
switch(config)# interface lag100  
switch(config-if)# sflow
```

Disabling sFlow on interface **lag100**:

```
switch(config)# interface lag100  
switch(config-if)# no sflow
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config config-if	Administrators or local user group members with execution rights for this command.

sflow agent-ip

```
sflow agent-ip <IP-ADDR>
no sflow agent-ip [<IP-ADDR>]
```

Description

Defines the IP address of the sFlow agent to use in sFlow datagrams. This address must be defined for sFlow to function. HPE recommends that the address:

- can uniquely identify the switch
- is reachable by the sFlow collector
- does not change with time

The **no** form of this command deletes the IP address of the sFlow agent. This causes sFlow to stop working and no datagrams will be sent to the sFlow collector.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. The agent address is used to identify the switch in all sFlow datagrams sent to sFlow collectors. It is usually set to an IP address on the switch that is reachable from an sFlow collector.

Examples

Setting the agent address to **10.10.10.100**:

```
switch(config)# sflow agent-ip 10.0.0.100
```

Setting the agent address to **2001:0db8:85a3:0000:0000:8a2e:0370:7334**:

```
switch(config)# sflow agent-ip 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Removing the address configuration from the switch, which results in sFlow being disabled:

```
switch(config)# no sflow agent-ip
```




For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow collector

```
sflow collector <IP-ADDR> [port <PORT>] [vrf <VRF>]  
no sflow collector <IP-ADDR> [port <PORT>] [vrf <VRF>]
```

Description

Defines a collector to which the sFlow agent sends data. Up to three collectors can be defined. At least one collector should be defined, and it must be reachable from the switch for sFlow to work.

Parameter	Description
collector <IP-ADDR>	Specifies the IP address of a collector in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255, or IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
port <PORT>	Specifies the UDP port on which to send information to the sFlow collector. Range: 0 to 65536. Default: 6343.
vrf <VRF>	Specifies the VRF on which to send information to the sFlow collector. The VRF must be defined on the switch. If no VRF is specified, the default VRF (default) is used.

Example

Defining a collector with IP address **10.10.10.100** on UDP port **6400**:

```
switch(config)# sflow collector 10.0.0.1 port 6400
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow disable

sflow disable

Description

Disables the sFlow agent, but retains any existing sFlow configuration settings. The settings become active if the sFlow agent is re-enabled.

Example

Disabling sFlow support:

```
switch(config)# sflow disable
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow header-size

sflow header-size <SIZE>
no sflow header-size [<SIZE>]

Description

Sets the sFlow header size in bytes.

The **no** form of this command sets the header size to the default value of 128.

Parameter	Description
header-size <SIZE>	Specifies the sFlow header size in bytes. Range: 64 to 256. Default: 128.

Examples

Setting the header size to **64** bytes:

```
switch(config)# sflow header-size 64
```

Setting the header size to the default value of **128** bytes:

```
switch(config)# no sflow header-size
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow max-datagram-size

```
sflow max-datagram-size <SIZE>
no sflow max-datagram-size [<SIZE>]
```

Description

Sets the maximum number of bytes that are sent in one sFlow datagram.

The **no** form of this command sets maximum number of bytes to the default value of 1400.

Parameter	Description
max-datagram-size <SIZE>	Specifies the maximum datagram size in bytes. Range: 1 to 9000. Default: 1400.

Examples

Setting the datagram size to **1000** bytes:

```
switch(config)# sflow max-datagram-size 1000
```

Setting the header size to the default value of **1400** bytes:

```
switch(config)# no sflow max-datagram-size
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow mode

```
sflow mode {ingress | egress | both}  
no sflow mode {ingress | egress | both}
```

Description

Sets the sFlow sampling mode. The default mode is ingress.

The no form of the command sets the sampling mode to ingress. Executing the no form of the command with the ingress option will have no impact as ingress is the default mode.

Parameter	Description
ingress	Samples only ingress traffic.
egress	Samples only egress traffic.
both	Samples both ingress and egress traffic.

Examples

Setting the sFlow mode to only sample egress traffic:

```
switch# configure terminal  
switch(config)# sflow mode egress
```

Setting the sFlow mode to only sample ingress traffic:

```
switch# configure terminal
switch(config)# sflow mode ingress
```

Setting the sFlow mode to sample both sample ingress and egress traffic:

```
switch# configure terminal
switch(config)# sflow mode both
```

Resetting the sFlow sampling mode to the default of ingress from previously configured mode of egress:

```
switch# configure terminal
switch(config)# no sflow mode egress
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command enabled on the 8320, 8325, 9300, and 10000 Switch Series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

sflow polling

```
sflow polling <INTERVAL>
no sflow polling [<INTERVAL>]
```

Description

Defines the global polling interval for sFlow in seconds.

The **no** form of this command sets the polling interval to the default value of 30 seconds.

Parameter	Description
<INTERVAL>	Specifies the polling interval in seconds. Range: 10 to 3600. Default: 30.

Examples

Setting the polling interval to 10:

```
switch(config)# sflow polling 10
```

Setting the polling interval to the default value.

```
switch(config)# no sflow polling
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

sflow sampling

```
sflow sampling <RATE>  
no sflow sampling [<RATE>]
```

Description

Defines the global sampling rate for sFlow in number of packets. The default sampling rate is 4096, which means that one in every 4096 packets is sampled. A warning message is displayed when the sampling rate is set to less than 4096 and proceeds only after user confirmation.

The **no** form of this command sets the sampling rate to the default value of 4096.

Parameter	Description
sampling <RATE>	Specifies the sampling rate. Range: 1 to 1000000000. Default: 4096.

Examples

Setting the sampling rate to **5000**:

```
switch(config)# sflow sampling 5000
```

Setting the sampling rate to the default:

```
switch(config)# no sflow sampling
```

Setting the sampling rate to **1000**:

```
switch(config)# sflow sampling 1000
Setting the sFlow sampling rate lower than 4096 is not recommended and might
affect system performance.
Do you want to continue [y/n]? y
switch(config)#
```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show sflow

```
show sflow [interface <INTERFACE-NAME>] [vsx-peer]
```

Description

Shows sFlow configuration settings and statistics for all interfaces, or for a specific interface. It also displays the current status of sFlow on the device and reports any errors that require attention.



If sFlow is enabled on the interfaces associated with a lag interface, then the interfaces will not be shown as separate entries under `sFlow enabled on Interface` in the output. Only the associated lag interface will have an entry in the column.

Parameter	Description
interface <INTERFACE-NAME>	Specifies the name of an interface on the switch.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing sFlow information for all interfaces:

```
switch# show sflow
```

```

sFlow Global Configuration
-----
sFlow                               enabled
Collector IP/Port/Vrf               10.0.0.2/6343/default
                                   10.0.0.3/6400/default
Agent Address                       10.0.0.1
Sampling Rate                       1024
Polling Interval                    30
Header Size                         128
Max Datagram Size                   1400
Sampling Mode                       ingress

sFlow Status
-----
Running - Yes

sFlow enabled on Interfaces:
-----
1/1/2
1/1/3
lag100

sFlow Statistics
-----
Number of Ingress Samples           200
Number of Egress Samples            120

```

Showing sFlow information for interface **1/1/1**:

```

switch# show sflow interface 1/1/1
sFlow configuration - Interface 1/1/1
-----
sFlow                               enabled
Sampling Rate                       1024
Sampling Mode                       both
Number of Ingress Samples            81
Number of Egress Samples             20
sFlow Sampling Status                success

```

Showing sFlow information for interface **lag 10**:

```

switch# show sflow interface lag 10
sFlow Configuration - Interface lag10
-----
sFlow                               enabled
Sampling Rate                       4096
Sampling Mode                       both
Number of Ingress Samples            0
Number of Egress Samples            0
sFlow Sampling Status                error

Sampling Status on LAG members
-----
Intf 1/1/2                          no agent
Intf 1/1/3                          no agent

```



For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command output updated to display <code>Sampling Mode</code> , Number of Ingress Samples , and Number of Egress Samples for 8320, 8325, 9300, and 10000 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

event-trap-disable

```
event-trap-disable <EVENT-IDS>
no event-trap-disable <EVENT-IDS>
```

Description

Disables the notification of specific events to be sent as traps to the SNMP management stations. Event traps are enabled by default.

The **no** form of this command enables the notification of events to be sent as traps.

Parameter	Description
<EVENT-IDS>	Specifies the comma-separated event IDs. Maximum: 20.

Examples

Disabling event traps:

```
switch(config)# event-trap-disable
```

Re-enabling event traps:

```
switch(config)# no event-trap-disable
```

Disabling event traps 403 and 404:

```
switch(config)# event-trap-disable 403,404
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

event-trap-enable

event-trap-enable
no event-trap-enable

Description

Enables the notification of events to be sent as traps to the SNMP management stations. It is enabled by default.

The **no** form of this command disables the event traps.

Examples

Enabling the event traps:

```
switch(config)# event-trap-enable
```

Disabling the event traps:

```
switch(config)# no event-trap-enable
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

lldp trap enable

lldp trap enable
no lldp trap enable

Description

Enables sending SNMP traps for LLDP related events from a particular interface. LLDP trap generation is enabled by default on all the interfaces and has to be disabled for interfaces on which traps are not required to be generated.

The **no** form of this command disables the LLDP trap generation.



LLDP trap generation is disabled by default at the global level and must be enabled before any LLDP traps are sent.

Examples

Enabling LLDP trap generation on global level:

```
switch(config)# lldp trap enable
```

Enabling LLDP trap generation on interface level:

```
switch(config-if)# lldp trap enable
```

Disabling LLDP trap generation on global level:

```
switch(config)# no lldp trap enable
```

Disabling LLDP trap generation on interface level:

```
switch(config-if)# no lldp trap enable
```

Displaying LLDP global configuration:

```
switch# show lldp configuration
```

LLDP Global Configuration

=====

```
LLDP Enabled           : No
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : No
```

TLVs Advertised

=====

```
Management Address
Port Description
Port VLAN-ID
System Description
System Name
```

LLDP Port Configuration

=====

PORT	TX-ENABLED	RX-ENABLED	INTF-TRAP-ENABLED
1/1/1	Yes	Yes	Yes
1/1/2	Yes	Yes	Yes
1/1/3	Yes	Yes	Yes
1/1/4	Yes	Yes	Yes

1/1/5	Yes	Yes	Yes
1/1/6	Yes	Yes	Yes
.....			
.....			
mgmt	Yes	Yes	Yes

Displaying LLDP Configuration for the interface:

```
switch# show lldp configuration 1/1/1
```

LLDP Global Configuration

```
=====
```

```
LLDP Enabled           : Yes
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : No
```

LLDP Port Configuration

```
=====
```

PORT	TX-ENABLED	RX-ENABLED	INTF-TRAP-ENABLED
1/1/1	Yes	Yes	Yes

Displaying LLDP Configuration for the management interface:

```
switch# show lldp configuration mgmt
```

LLDP Global Configuration

```
=====
```

```
LLDP Enabled           : Yes
LLDP Transmit Interval : 30
LLDP Hold Time Multiplier : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval : 2
LLDP Trap Enabled      : Yes
```

LLDP Port Configuration

```
=====
```

PORT	TX-ENABLED	RX-ENABLED	INTF-TRAP-ENABLED
mgmt	Yes	Yes	Yes



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release

Modification

10.07 or earlier

--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code> and <code>config-if</code>	Administrators or local user group members with execution rights for this command.

mac-notify traps

```
mac-notify traps {aged | learned | moved | removed}
no mac-notify traps {aged | learned | moved | removed}
```

Description

Configures a Layer 2 or VXLAN interface to generate SNMP trap notifications for up to four different types of MAC address related events on the trunk or access in physical or lag interfaces.

MAC notification trap addition to or removal from an interface can be in any combination, quantity, or order. The addition of existing configured traps or removal of non-configured traps will be accepted and ignored.



The **mac-notify** feature must be enabled globally for any interface configurations to generate SNMP traps. Enabling **mac-notify traps** may impact the system performance on networks with a large number of mac-notify events.

The **no** form of this command removes the traps from the interface.

Parameter	Description
<code>aged</code>	Notifies when a MAC address aged out on the interface.
<code>learned</code>	Notifies when a MAC address is learned on the interface.
<code>moved</code>	Notifies when a MAC address moved from the interface.
<code>removed</code>	Notifies when a MAC address is removed from the interface.

MAC notification cannot be configured on a Layer 3 (routing) interface. A Layer 2 interface that is changed to a Layer 3 interface through the `routing` command will discard any existing MAC notification configurations.



When MACs are learned on VXLAN tunnels or **port-access port-security** enabled ports, the move scenario is handled by the EVPN/port-access feature respectively. It performs the move by deleting the MAC from the old port and installing it on the new port. In this scenario, MAC trap notifications, if enabled, will reflect that by producing **removed** and **learned** notifications.

Usage

- MAC notify trap will not generate for static MACs.
- vsx-sync** is not supported. You must enable the MAC notify traps explicitly on secondary to ensure the traps are generated.
- For EVPN MAC move between the following interfaces, the respective event types are produced (not always removed or learned)

- Port to port: **moved**
- Port to tunnel: **removed/learned**
- Tunnel to port: **removed/learned**
- Tunnel to Tunnel: **moved**

Examples



MAC notification types and the associated events only apply to Layer 2 and VXLAN interfaces, hence routing might need to be disabled on the relevant interfaces.

Enable MAC notification traps within the SNMP module at a global level:

```
switch(config)# snmp-server trap

aaa-server-reachability-status  Enable SNMP trap for AAA server reachability
status
configuration-changes           Enable configuration changes traps
cpu-utilization                 Enable high CPU utilization traps
link-status                     Enable link status traps for all physical
interfaces
mac-notify                      Enable MAC table change notification traps
memory-utilization              Enable high memory utilization traps
module                          Enable module event traps
port-security                   Enable port-security violation traps.
                                (Default: enable)
rmon-events                     Enable RMON event traps
snmp                            Enable snmp traps
```

For more information, see [snmp-server trap mac-notify](#).

Enabling the traps on an L2 interface:

```
switch(config)# interface 1/1/1
switch(config-if)# mac-notify traps learned
1/1/1 is not an L2 interface or tunnel
switch(config-if)# no routing
switch(config-if)# mac-notify traps learned removed
switch(config-if)# mac-notify traps moved
switch(config-if)# mac-notify traps aged
```

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# mac-notify traps learned removed
```

```
switch(config)# interface lag101
switch(config-if)# mac-notify traps removed
```

Disabling the `learned` and `removed` traps from the interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no mac-notify traps learned removed
```

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# no mac-notify traps learned removed
```

Enable sending SNMP notifications for MAC table changes:

```
switch(config-vxlan-if)# mac-notify traps
aged          Notify when a MAC address aged out on the interface
learned       Notify when a MAC address was learned on the interface
moved         Notify when a MAC address moved from the interface
removed       Notify when a MAC address was removed from the interface
switch(config-vxlan-if)# mac-notify traps learned aged removed moved
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.13.1000	Support for SNMP MAC notify traps on VXLAN tunnels.
10.10	Support for port access features with mac-notify added.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command. Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

rmon alarm

```
rmon alarm index <INDEX> snmp-oid <SNMP-OID> rising-threshold <RISING-THRESHOLD>
    falling-threshold <FALLING-THRESHOLD> [sample-interval <SAMPLE-INTERVAL>] [sample-
type <ABSOLUTE|DELTA>]
no rmon alarm [index <INDEX>]
```

Description

Stores configuration entries in an alarm table that defines the sample interval, sample-type, and threshold parameters for an SNMP MIB object. Only the SNMP MIB objects that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge32, or TimeTicks) will be monitored.

The **no** form of this command removes all RMON alarms and allows you to specify an index to remove a particular RMON alarm.

Parameter	Description
index <INDEX>	Specifies the RMON alarm index. Range: 1 to 20.
snmp-oid <SNMP-OID>	Specifies the SNMP MIB object to be monitored by RMON.
rising-threshold <RISING-THRESHOLD>	Specifies the upper threshold value for the RMON alarm.
falling-threshold <FALLING-THRESHOLD>	Specifies the falling threshold value for the RMON alarm. The falling threshold must be less than the rising threshold.
sample-interval <SAMPLE-INTERVAL>	Sample interval in seconds. Default: 30.
sample-type <ABSOLUTE DELTA>	Specifies the method of sampling of the SNMP MIB object. Default: Absolute.

Examples

Configuring RMON for the MIB object **ifOutErrors.15** with an index **1**, rising threshold of **2147483647** and falling threshold of **-2134** using **absolute** sampling for a sample interval of **100** seconds:

```
switch(config)# rmon alarm index 1 snmp-oid ifOutErrors.15 rising-threshold
2147483647
falling-threshold -2134 sample-type absolute sample-interval 100
```

Removing RMON alarm with the index 5:

```
switch(config)# no rmon alarm index 5
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

rmon alarm {enable | disable} {index | all}

```
rmon alarm {enable | disable} {index <INDEX> | all}
no rmon alarm [enable | disable] [index <INDEX> | all]
```

Description

Enables and disables the RMON alarm and its index. RMON alarm is enabled by default.

Parameter	Description
enable	Enables the RMON alarm index
disable	Disables the RMON alarm index.
index <INDEX>	Specifies the RMON alarm index. Range: 1 to 20.
all	Specifies all the RMON alarms.

Examples

Enabling or disabling all the RMON alarm:

```
switch(config)# rmon alarm enable all
switch(config)# rmon alarm disable all
```

Enabling or disabling RMON alarm by index:

```
switch(config)# rmon alarm enable index 1
switch(config)# rmon alarm disable index 1
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show configuration-changes trap

```
show configuration-changes trap
```

Description

Shows the SNMP configuration changes trap settings.

Example

Showing the SNMP configuration changes trap:

```
switch# show configuration-changes trap

SNMP Configuration changes trap : Enabled
^^^
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-notify

```
show mac-notify
```

Description

Displays whether the MAC notification feature in the SNMP module is enabled or not. It also displays the trap notification types configured on the Layer 2 ports in the system.

Examples

Showing the MAC notification configuration on all configured ports in the system:

```
switch# show mac-notify

MAC notification global setting : Enabled

Port          Enabled Traps
-----
1/1/1         aged learned moved
1/1/5         moved
lag101        removed
lag104        aged learned moved removed
...
...
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mac-notify port

show mac-notify [port <PORTS>]

Description

Displays the MAC notification configuration on a range of ports.

Parameter	Description
[port <PORTS>]	Specifies a port, range of ports, or list of ports.

Examples

Showing the MAC notification configuration on a range of ports:

```
switch(config)# show mac-notify port 1/1/1,1/1/3,1/1/5,lag101-lag104

MAC notification global Setting: Enabled

Port          Enabled Traps
-----
1/1/1         aged learned moved
1/1/3         --
1/1/5         moved
lag101        removed
lag102        --
lag103        --
lag104        aged learned moved removed
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show rmon alarm

show rmon alarm [index <INDEX>]

Description

Displays the RMON alarm configurations.

Parameter	Description
index <INDEX>	Specifies the RMON alarm index. Range: 1 to 20.

Examples

Showing all RMON alarm configurations:

```
switch# show rmon alarm
Index          : 1
Enabled        : true
Status         : valid
MIB object     : ifOutErrors.15
Sample type    : delta
Sampling interval : 6535 seconds
Rising threshold : 100
Falling threshold : 10
Last sampled value : 0
Last sample time : 2020-09-21 05:58:11

Index          : 3
Enabled        : true
Status         : invalid
MIB object     : IF-MIB::ifDescr.19
Sample type    : absolute
Sampling interval : 10000 seconds
Rising threshold : 4000
Falling threshold : 10
Last sampled value : 0
```

Showing RMON alarm with alarm index 1:

```
switch# show rmon alarm index 1
Index          : 1
Enabled        : true
Status         : valid
MIB object     : ifOutErrors.15
Sample type    : delta
Sampling interval : 6535 seconds
Rising threshold : 100
Falling threshold : 10
Last sampled value : 0
Last sample time : 2020-06-21 05:58:11
```

Showing disabled RMON alarm information:

```
switch# show rmon alarm
Index          : 1
Enabled        : false
Status         : valid
MIB object     : ifOutErrors.15
Sample type    : delta
Sampling interval : 6535 seconds
Rising threshold : 100
Falling threshold : 10
Last sampled value : 0
Last sample time : 2020-09-21 05:58:11

Index          : 3
Enabled        : false
Status         : invalid
MIB object     : IF-MIB::ifDescr.19
Sample type    : absolute
Sampling interval : 10000 seconds
Rising threshold : 4000
Falling threshold : 10
Last sampled value : 0
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show snmp agent-port

show snmp agent-port

Description

Displays SNMP agent UDP port number.

Example

Displaying SNMP agent UDP port number:

```
switch# show snmp agent-port
SNMP agent port : 161
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp community

show snmp community

Description

Displays a list of all configured SNMPv1/v2c communities.

Usage

When a user creates a custom community before enabling an SNMP agent, AOS-CX automatically removes the default **public** community from the system.

Example

Displaying a list of all configured SNMPv1/v2c communities:

```
switch#show snmp community
```

```
SNMP-COMMUNITIES
```

```
-----  
Community      Access-level  ACL Name    ACL Type    View  
-----  
private         ro           my_acl      ipv4         view1  
private         ro           my_acl      ipv6         none  
private2        rw           new_Acl     ipv6         view2  
private3        rw           none        none         none
```

When the switch is configured to use [SNMPv3 only](#), the output of the **show snmp community** command displays the message **SNMP v1/v2c is disabled while snmpv3-only mode is configured**:

```
switch# show snmp community
```

```
-----  
-----  
Community      Access-level  ACL Name    ACL Type  
View
```

```
-----  
-----  
SNMP v1/v2c is disabled while snmpv3-only mode is configured
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.14	The output of this command now displays an error message when the switch is in SNMPv3-only mode.
10.10	Output has been updated with SNMP view details. A <i>View</i> column is added to the command output.
10.08	Added <i>ACL Type</i> column to the command output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show snmp system

```
show snmp system
```

Description

Displays SNMP description, location, and contact information.

Example

Displaying SNMP description, location, and contact information:

```
switch# show snmp system  
SNMP system information  
-----  
System description : Aggregation router  
System location   : Main lab  
System contact    : John Smith, Lab Admin
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp trap

show snmp trap

Description

Displays all configured SNMP traps/informs receivers.

Example

Displaying all configured SNMP trap and informs receivers:

```
switch# show snmp trap
```

HOST	PORT	TYPE	VER	COMMUNITY/USER	NAME	VRF	NOTIFICATION TYPES
-							
10.10.10.10	162	trap	v1	public		default	bgp
10.10.10.10	162	inform	v2c	public		default	bgp, ospf, fan,
mstp							
10.10.10.10	162	inform	v3	name		default	



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.14	Updated the example output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp views

show snmp views

Description

Displays the list of all the configured SNMP views.

Usage

The following table contains the status and its description of the configured SNMP views:

Status	Description
pending_validation	Default value that indicates SNMP view is yet to be validated.
operational	OID and mask validated.
invalid	Invalid OID/mask.
failed	Validation failed for reasons other than OID/mask.

Examples

Displaying the list of all the configured SNMP views:

```
switch# show snmp views
-----
SNMP MIB Views
-----
View      : new
OID Tree: sysUpTime.0
Mask      : ff
Type      : included
Status    : pending_validation

View      : admin
OID Tree: ifIndex.1
Mask      : ff:a0
Type      : included
Status    : operational

View      : user
OID Tree: sysb
Mask      : none
Type      : excluded
Status    : invalid

View      : admin
OID Tree: .1.3.6.1.2.1.1
Mask      : none
Type      : excluded
Status    : operational
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmp vrf

show snmp vrf

Description

Displays the VRF on which the SNMP agent service is running.

Example

Displaying SNMP services enabled on VRF:

```
switch#show snmp vrf
SNMP enabled VRF
-----
mgmt
default
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 context

show snmpv3 context

Description

Displays all configured SNMP contexts.

Examples

Displaying all configured SNMP contexts:

```
switch# show snmpv3 context
```

name	vrf	community
contextA	default	private
contextB	vrf_A	public

```
switch# show snmpv3 context
```

Name	vrf	Community	ype[Instance_id]
A	default	public	vrf

```
switch#
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 engine-id

```
show snmpv3 engine-id
```

Description

Displays the configured SNMPv3 snmp engine-id.

If the SNMPv3 engine-id is not configured, by default a unique engine-id is created by the switch using a combination of the enterprise OID value and the switch's mac address.

Example

Displaying the configured SNMPv3 engine-id:

```
switch# show snmpv3 engine-id
SNMP engine-id : 80:00:B8:5C:08:00:09:1d:de:a5
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 security-level

```
show snmpv3 security-level
```

Description

Displays the configured SNMPv3 security level.

Examples

Displaying the configured SNMPv3 security level:

```
switch# show snmpv3 security-level
SNMPv3 security-level : auth
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show snmpv3 users

```
show snmpv3 users
```

Description

Displays all configured SNMPv3 users.

For more details on the user enabled status, see [snmpv3 security-level](#).

Example

Displaying all configured SNMPv3 users:

```
switch# show snmpv3 users
```

User	AuthMode	PrivMode	Status	Context	Access-level	View
name	md5	none	Enabled	context2 context1 context3	ro	view1
name2	none	none	Disabled	none	ro	view2
name3	none	none	Disabled	none	ro	none



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Output has been updated with SNMP view details. A <i>View</i> column is added to the command output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

snmp-server agent-port

```
snmp-server agent-port <PORT>  
no snmp-server agent-port [<PORT>]
```

Description

Sets the UDP port number that the SNMP master agent uses to communicate. UDP port 161 is the default port.

The **no** form of this command sets the SNMP master agent port to the default value.

Parameter	Description
<PORT>	Specifies the UDP port number that the SNMP master agent will use. Range: 1 to 65535. Default: 161.

Examples

Setting the SNMP master agent port to **2000**:

```
switch(config)# snmp-server agent-port 2000
```

Resetting the SNMP master agent port to the default value:

```
switch(config-schedule)# no snmp-server agent-port 2000
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server community

```
snmp-server community <STRING>  
no snmp-server community <STRING>
```

Description

Adds an SNMPv1/SNMPv2c community string. A community string is like a password that controls read/write access to the SNMP agent. A network management program must supply this name when attempting to get SNMP information from the switch. A maximum of 10 community strings are supported. Once you create your own community string, the default community string (`public`) is deleted.

The **no** form of this command removes the specified SNMPv1/SNMPv2c community string. When no community string exists, a default community string with the value **public** is automatically defined.

Parameter	Description
<STRING>	Specifies the SNMPv1/SNMPv2c community string. Range: 1 to 32 printable ASCII characters, excluding space and question mark.

Subcommands

```
access-level {ro | rw}  
no access-level {ro | rw}
```

This subcommand changes the access level of the SNMP community. The default access level is read-only (**ro**).

The **no** form of this subcommand changes the access level of the community to default.

Parameter	Description
ro	Specifies Read-Only access with the SNMP community.
rw	Specifies Read-Write access with the SNMP community.

```
access-list {ip | ipv6} <ACL-NAME>  
no access-list {ip | ipv6} <ACL-NAME>
```

This subcommand associates an ACL with the SNMP community. If an ACL is not associated with the SNMP community, the default access is allowed for all the hosts.

The **no** form of this subcommand removes association of the ACL with the SNMP community.

Parameter	Description
ip	Specifies the IPv4 ACL type.
ipv6	Specifies the IPv6 ACL type.
<ACL-NAME>	Specifies the ACL name. It supports a maximum of 64 characters.

Examples

Setting the SNMPv1/SNMPv2c community string to **private**:

```
switch(config)# snmp-server community private
```

Removing SNMPv1/SNMPv2c community string **private**:

```
switch(config)# no snmp-server community private
```

Configuring the access level for the SMNP community to read-only:

```
switch(config-community)# access-level ro
```

Changing the access level of the SNMP community to default:

```
switch(config-community)# no access-level rw
```

Associating an IPv4 ACL named **my_acl** with the SMNP community:

```
switch(config-community)# access-list ip my_acl
```

Removing the associated IPv4 ACL named **my_acl** from the SNMP community:

```
switch(config-community)# no access-list ip my_acl
```

Configuration supported for SNMP ACL:


```

access-list ip ipv4_acl
  10 permit any 4.4.4.4 4.4.4.1
  20 permit any 3.3.3.3 3.3.3.1
access-list ipv6 ipv6_acl
  10 permit any 2001::2 2001::1
  20 permit any 3001::2 3001::1
snmp-server vrf default
snmp-server community my_comm_1
  access-list ip ipv4_acl
  access-list ipv6 ipv6_acl

```

Configuration not supported for SNMP ACL:

```

access-list ip ipv4_acl
  10 deny any 6.6.6.6 6.6.6.1
access-list ipv6 ipv6_acl
  10 deny any 6001::6 6000::1
snmp-server vrf default
snmp-server community my_comm_1
  access-list ip ipv4_acl
  access-list ipv6 ipv6_acl

```



hitcounts for SNMP ACL will not be incremented.

Example: `show access-list hitcounts ip all` will not show the hit count of SNMP ACL.



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.14	Replaced the ipv4 parameter with the ip parameter. The ipv4 parameter is deprecated.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config config-community	Administrators or local user group members with execution rights for this command.

snmp-server community view

```

snmp-server community <STRING> [view <VIEW-NAME>]
no snmp-server community <STRING> [view <VIEW-NAME>]

```

Description

Associates an SNMP MIB view with the SNMP community.

The **no** form of this command removes the associated SNMP MIB view from the SNMP community.

Parameter	Description
<STRING>	Specifies the SNMPv1/SNMPv2c community string. Range: 1 to 32 printable ASCII characters, excluding space and question mark.
<VIEW-NAME>	Specifies the view name for the SNMP MIB view. Accepts a maximum of 32 characters.

Examples

Configuring the SNMPv1/SNMPv2c community:

```
switch(config) # snmp-server community my_community
switch(config-community) #
```

Adding SNMP MIB view to the SNMP community:

```
switch(config-community) # view name1
```

Removing SNMP MIB view from the SNMP community:

```
switch(config-community) # no view name1
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config config-community	Administrators or local user group members with execution rights for this command.

snmp-server historical-counters-monitor

```
snmp-server historical-counters-monitor
no snmp-server historical-counters-monitor
```

Description

Enables the Remote Network Monitoring agent (**rmond**) to start collecting historical interface statistics. The **no** form of this command stops the historical interface statistics collection.

Example

Enabling the `rmond` agent to start historical interface statistics collection:

```
switch(config)# snmp-server historical-counters-monitor
```

Disabling the `rmond` agent to stop historical interface statistics collection:

```
switch(config)# no snmp-server historical-counters-monitor
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

snmp-server response-source

```
snmp-server response-source {interface <IF-NAME> | <IPv4-ADDRESS> | <IPv6-ADDRESS>} [vrf <VRF-NAME>]  
no snmp-server response-source {interface <IF-NAME> | <IPv4-ADDRESS> | <IPv6-ADDRESS>}  
[vrf <VRF-NAME>]
```

Description

Configures the source interface or IP address for sending SNMP responses. Each SNMP can independently have its own unique response source IP address.

The **no** form of this command removes the source interface name or IP address for sending SNMP responses.

- It is recommended to use the loopback interface or ip address of the loopback interface as the response source. If a device does not support a loopback interface, then configure SVI interface or SVI IP address as the response source.
- The active gateway IP address cannot be configured as the response source.
- It is recommended to limit the maximum number of response source to five.
- The interface used for the response source should be in the up state. If the interface is down, the default source IP will be used.
- The use of **udp6** is mandatory for IPv6 SNMP operations. For example, you can use the following syntax:
snmpwalk -v2c -c public -m ALL udp6:[2100::2] .1.3.6.1.2.1.1.



Parameter	Description
<code>interface <IF-NAME></code>	Specifies the source interface name. The interface can be a physical interface, loopback interface, or VLAN interface.
<code><IPv4-ADDRESS></code>	Specifies the IPv4 address of the source interface for the SNMP response.
<code><IPv6-ADDRESS></code>	Specifies the IPv6 address of the source interface for the SNMP response.
<code>vrf <VRF-NAME></code>	Specifies the VRF name associated to the source interface for the SNMP response.

Examples

Configuring a response source for the interface **1/1/12**:

```
switch(config)# snmp-server response-source interface 1/1/12 vrf red
```

Configuring a response source for interface **loopback10**:

```
switch(config)# snmp-server response-source interface loopback10 vrf red
```

Configuring a response source for the IPv4 address **10.0.0.1**:

```
switch(config)# snmp-server response-source 10.0.0.1 vrf sample
```

Configuring a response source for the IPv6 address **2001::1**:

```
switch(config)# snmp-server response-source 2001::1 vrf default
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.13	Added support for IPv6 address.
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

snmp-server snmpv3-only

```
snmp-server snmpv3-only
no snmp-server snmpv3-only
```

Description

Accepts SNMPv3 messages only, SNMPv1 and SNMPv2c will be disabled. By default SNMPv1, SNMPv2c and SNMPv3 will all be enabled.

The **no** form of this command restores the default setting and reenables SNMPv1 and SNMPv2c .

Examples

Configuring SNMPv3 messages only, and disabling SNMPv1 and SNMPv2c:

```
switch(config)# snmp-server snmpv3-only
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server host

```
snmp-server host <IPv4-ADDR | IPv6-ADDR> trap version <VERSION> [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>] [notification-type <NOTIFICATION-TYPE>]
no snmp-server host <IPv4-ADDR | IPv6-ADDR> trap version <VERSION> [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>] [notification-type <NOTIFICATION-TYPE>]
```

```
snmp-server host <IPv4-ADDR | IPv6-ADDR> inform version v2c [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>] [notification-type <NOTIFICATION-TYPE>]
no snmp-server host <IPv4-ADDR | IPv6-ADDR> inform version v2c [community <STRING>]
[port <UDP-PORT>] [<VRF-NAME>] [notification-type <NOTIFICATION-TYPE>]
```

```
snmp-server host <IPv4-ADDR | IPv6-ADDR> [trap version v3 | inform version v3] user
<NAME> [port <UDP-PORT>] [<VRF-NAME>] [notification-type <NOTIFICATION-TYPE>]
no snmp-server host <IPv4-ADDR | IPv6-ADDR> [trap version v3 | inform version v3] user
<NAME> [port <UDP-PORT>] [<VRF-NAME>] [notification-type <NOTIFICATION-TYPE>]
```

Description

Configures a trap/informs receiver to which the SNMP agent can send SNMP v1/v2c/v3 traps or v2c informs. A maximum of 30 SNMP traps/informs receivers can be configured.

The **no** form of this command removes the specified trap/inform receiver.



Avoid configuring the same receiver for both SNMP traps and informs on the same UDP port for v1, v2, and v3.

Parameter	Description
<code><IPv4-ADDR></code>	Specifies the IP address of a trap receiver in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. You can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100 .
<code><IPv6-ADDR></code>	Specifies the IP address of a trap receiver in IPv6 format (x:x::x:x).
<code>trap version <VERSION></code>	Specifies the trap notification type for SNMPv1, v2c or v3. Available options are: v1 , v2c or v3 .
<code>inform version v2c</code>	Specifies the inform notification type for SNMPv2c.
<code>trap version v3</code>	Specifies the trap notification type for SNMPv3.
<code>user <NAME></code>	Specifies the SNMPv3 user name to be used in the SNMP trap notifications.
<code>community <STRING></code>	Specifies the name of the community string to use when sending trap notifications. Range: 1 - 32 printable ASCII characters, excluding space and question mark. Default: public .
<code><UDP-PORT></code>	Specifies the UDP port on which notifications are sent. Range: 1 - 65535. Default: 162.
<code><VRF-NAME></code>	Specifies the VRF on which the SNMP agent listens for incoming requests.
<code><notification-type></code>	Specifies the type of notification to be sent to the trap receiver. If no type is specified, all notifications are sent. The supported notification types are: ▪ aaa-server ▪ alarm ▪ bgp ▪ card ▪ config ▪ entity ▪ fan ▪ interface ▪ lldp ▪ loop-protect ▪ mac-notify ▪ mstp ▪ mvrp ▪ ospf ▪ ospfv3 ▪ port-security ▪ power ▪ power-ethernet ▪ rmon

Parameter	Description
	■ rpvst ■ stp ■ temperature ■ vrrp ■ vsf ■ vsx

Examples

```

switch(config)# snmp-server host 10.10.10.10 trap version v1
switch(config)# no snmp-server host 10.10.10.10 trap version v1
switch(config)# snmp-server host a:b::c:d trap version v1
switch(config)# no snmp-server host a:b::c:d trap version v1
switch(config)# snmp-server host 10.10.10.10 trap version v2c community public
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
switch(config)# snmp-server host a:b::c:d trap version v2c community public
switch(config)# no snmp-server host a:b::c:d trap version v2c community public
switch(config)# snmp-server host 10.10.10.10 trap version v2c community public
port 5000
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
port 5000
switch(config)# snmp-server host 10.10.10.10 trap version v2c community public
port 5000 vrf default
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
port 5000 vrf default
switch(config)# snmp-server host a:b::c:d trap version v2c community public port
5000
switch(config)# no snmp-server host a:b::c:d trap version v2c community public
port 5000
switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community
public
switch(config)# snmp-server host a:b::c:d inform version v2c community public
switch(config)# no snmp-server host a:b::c:d inform version v2c community public
switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
port 5000
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community
public port 5000
switch(config)# snmp-server host 10.10.10.10 inform version v2c community public
port 5000 vrf default
switch(config)# no snmp-server host 10.10.10.10 inform version v2c community
public port 5000 vrf default
switch(config)# snmp-server host a:b::c:d inform version v2c community public port
5000
switch(config)# no snmp-server host a:b::c:d inform version v2c community public
port 5000
switch(config)# snmp-server host 10.10.10.10 trap version v3 user Admin
switch(config)# no snmp-server host 10.10.10.10 trap version v3 user Admin
switch(config)# snmp-server host a:b::c:d trap version v3 user Admin
switch(config)# no snmp-server host a:b::c:d trap version v3 user Admin
switch(config)# snmp-server host 10.10.10.10 trap version v3 user Admin port 2000
switch(config)# no snmp-server host 10.10.10.10 trap version v3 user Admin port
2000
switch(config)# snmp-server host a:b::c:d trap version v3 user Admin port 2000
switch(config)# no snmp-server host a:b::c:d trap version v3 user Admin port 2000

```

SNMP trap notification type examples:

```

switch(config)# snmp-server host 10.10.10.10 trap version v2c community public
notification-type bgp fan interface power entity
switch(config)# no snmp-server host 10.10.10.10 trap version v2c community public
notification-type bgp
switch(config)# snmp-server host a:b::c:d inform version v3 user Admin
notification-type bgp fan interface power-ethernet
switch(config)# no snmp-server host a:b::c:d inform version v3 user Admin
notification-type bgp interface
switch(config)# snmp-server host a:b::c:d inform version v3 user Admin
notification-type ?
aaa-server          Sends AAA notifications.
alarm               Sends Alarm notifications.
bgp                 Sends Border Gateway Protocol (BGP) state change notifications.
card                Sends Card notifications.
config              Sends Configuration change notifications.
entity              Sends Entity notifications.
fan                 Sends Fan notifications.
interface           Sends Interface notifications.
lldp                Sends Link Layer Discovery Protocol (LLDP) notifications.
loop-protect        Sends Loop Protect notifications.
mac-notify          Sends MAC Notify notifications.
mstp                Sends Multiple Spanning Tree Protocol (MSTP) notifications.
mvrp                Sends Multiple VLAN Registration Protocol (MVRP) notifications.
ospf                Sends Open Shortest Path First (OSPFv2) notifications.
ospfv3              Sends Open Shortest Path First version 3 (OSPFv3) notifications.
port-security       Sends Port Security notifications.
power               Sends Power notifications.
power-ethernet      Sends Power over Ethernet (PoE) notifications.
rmon                Sends Remote Network Monitoring (RMON) notifications.
rpvst               Sends Rapid Per VLAN Spanning Tree (RPVST) notifications.
snmp                Sends Sends Simple Network Management Protocol (SNMP)
notifications.
stp                 Sends Spanning Tree Protocol (STP) notifications.
temperature         Sends Temperature notifications.
vrrp                Sends Virtual Router Redundancy Protocol (VRRP) notifications.
vsf                 Sends Virtual Switching Framework (VSF) notifications.
vsx                 Sends Virtual System Extension (VSX) notifications.

```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server system-contact


```
snmp-server system-contact <INFO>
no snmp-server system-contact [<INFO>]
```

Description

Sets SNMP contact information.

The **no** form of this command removes the SNMP contact information.

Parameter	Description
<INFO>	Specifies SNMP contact information. Range: 1 to 128 printable ASCII characters, except for question mark (?).

Examples

Defines SNMP contact information to be **John Smith, Lab Admin**:

```
switch(config)# snmp-server system-contact John Smith, Lab Admin
```

Removes SNMP contact information:

```
switch(config)# no snmp-server system-contact
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server system-description

```
snmp-server system-description <DESCRIPTION>
no snmp-server system-description
```

Description

Sets the SNMP system description.

The **no** form of this command removes the SNMP system description.

Parameter	Description
<i><DESCRIPTION></i>	Specifies the SNMP system description. Typical content to include would be the full name and version of the following: - Hardware type of the system - Software operating system - Networking software Range: 1 to 64 printable ASCII characters, except for the question mark (?).

Examples

Defines the SNMP system description to be **mainSwitch**:

```
switch(config) # snmp-server system-description mainSwitch
```

Removes the SNMP system description:

```
switch(config) # no snmp-server system-description mainSwitch
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server system-location

```
snmp-server system-location <INFO>
no snmp-server system-location
```

Description

Sets the SNMP location information.

The **no** form of this command removes the SNMP location information.

Parameter	Description
<i><INFO></i>	Specifies the SNMP location information. Range: 1 to 128 printable ASCII characters, except for the question mark (?).

Examples

Defines the SNMP location information to be **Main Lab**:

```
switch(config)# snmp-server system-location Main Lab
```

Removes the SNMP location information:

```
switch(config)# no snmp-server system-location
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap

```
snmp-server trap {cpu-utilization | memory-utilization | rmon-events}  
no snmp-server trap {cpu-utilization | memory-utilization | rmon-events}
```

Description

Enables the SNMP traps. The SNMP traps are enabled by default.

The **no** form of this command disables the SNMP traps.

Parameter	Description
cpu-utilization	Enables the CPU utilization traps.
memory-utilization	Enables the memory utilization traps.
rmon-events	Enables the RMON event traps.

Examples

Enabling the SNMP traps:

```
switch(config)# snmp-server trap cpu-utilization  
switch(config)# snmp-server trap memory-utilization  
switch(config)# snmp-server trap rmon-events
```

Disabling the SNMP traps:

```
switch(config)# no snmp-server trap cpu-utilization
switch(config)# no snmp-server trap memory-utilization
switch(config)# no snmp-server trap rmon-events
```

Displaying the SNMP trap configuration:

```
switch(config)# show running-config all | inc snmp
snmp-server trap rmon-events
snmp-server trap cpu-utilization
snmp-server trap memory-utilization
```

Displaying CPU and Memory usage:

```
switch(config)# show system
Hostname           : XXXX
System Description : XX.10.07.0001CI
System Contact     :
System Location    :
Vendor            : Aruba
Product Name       : JLXXXX XXXX Base Chassis/3xFT/18xFans/Cbl Mgr/X462 Bundle
Chassis Serial Nbr : SG6Z009068
Base MAC Address   : f40343-806400
AOS-CX Version    : XX.10.07.0001CI
Time Zone          : UTC
Up Time           : 8 minutes
CPU Util (%)       : 1
Memory Usage (%)   : 10
```



cpu-utilization and **memory-utilization** are not supported in 4100i, 6000 and 6100 switch series. For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap aaa-server-reachability-status

```
snmp-server trap aaa-server-reachability-status
no snmp-server trap aaa-server-reachability-status
```

Description

Enables the SNMP trap for AAA server status. When enabled, traps are sent whenever AAA server (RADIUS, TACACS) status changes from reachable to unreachable and vice versa.

The **no** form of this command disables sending SNMP trap for AAA server status.

Examples

Enabling the SNMP trap for AAA server status:

```
switch(config)# snmp-server trap aaa-server-reachability-status
```

Disabling the SNMP trap for AAA server status:

```
switch(config)# no snmp-server trap aaa-server-reachability-status
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced on 4100i, 6000, 6100, 8100, 8320, 8325, 8360, 8400, 9300, and 10000 switches.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap configuration-changes

```
snmp-server trap configuration-changes  
no snmp-server trap configuration-changes
```

Description

Enables sending SNMP traps whenever the configuration changes. Configuration trap generation is disabled by default.

The **no** form of this command disables sending SNMP traps for configuration changes.

Parameter	Description
configuration-changes	Specifies SNMP traps for configuration changes.

Examples

Enabling the SNMP traps for configuration changes:

```
switch(config)# snmp-server trap configuration-changes
```

Disabling the SNMP traps for configuration changes:

```
switch(config)# no snmp-server trap configuration-changes
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap mac-notify

```
snmp-server trap mac-notify  
no snmp-server trap mac-notify
```

Description

Enables the MAC notification traps within the SNMP module at a global level. When enabled, traps are sent for interfaces that are configured for MAC notification events.

The **no** form of this command disables sending MAC notification traps at a global level. When disabled, existing **mac-notify** interface configuration is preserved but MAC notification events on configured interfaces will not cause SNMP traps to be transmitted.

Examples

Enabling the SNMP MAC notification feature in the system globally:

```
switch(config)# snmp-server trap mac-notify
```

Disabling the SNMP MAC notification feature in the system globally:

```
switch(config)# no snmp-server trap mac-notify
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap snmp

```
snmp-server trap snmp {authentication | coldstart | warmstart} [vrf <VRF_NAME>]
no snmp-server trap snmp {authentication | coldstart | warmstart} [vrf <VRF_NAME>]
```

Description

Enables SNMPv2 MIB traps. The SNMPv2 traps are disabled by default.

The **no** form of this command disables the SNMPv2 MIB traps.

SNMPv2 MIB supports the following traps:

- **authentication**: Authentication trap is sent when the SNMP server receives a protocol message that is not properly authenticated.
- **coldstart**: A coldstart trap is sent when the switch reboots.
- **warmstart**: A warmstart trap is sent when there is a user intervention to enable or disable the SNMP service on the switch.



SNMPv2 Authentication traps do not support source IP configuration.

Parameter	Description
authentication	Enables the authentication traps.
coldstart	Enables the coldstart traps.
warmstart	Enables the warmstart traps.
<VRF_NAME>	Specifies the VRF name. Enables the SNMPv2 traps for a VRF.

Examples

Enabling all SNMPv2 traps:

```
switch(config)# snmp-server trap snmp
```

Enabling only SNMPv2 authentication traps:

```
switch(config)# snmp-server trap snmp authentication
```

Disabling all SNMP traps:

```
switch(config)# no snmp-server trap snmp
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap-source interface vrf

```
snmp-server trap-source {interface <IF-NAME> | <IPv4-Address> | <IPv6-Address>} [vrf <VRF-NAME>]
```

```
no snmp-server trap-source {interface <IF-NAME> | <IPv4-Address> | <IPv6-Address>} [vrf <VRF-NAME>]
```

Description

Configures SNMP trap source interface or IP address for a VRF.

The **no** form of this command removes the SNMP **trap-source** configuration for a VRF.

Parameter	Description
<IF-NAME>	Specifies the source interface name. Interface name can be physical interface, loopback interface, LAG interface, or VLAN interface.
<IPv4-Address>	Specifies the IPv4 address of source interface for the SNMP trap.
<IPv6-Address>	Specifies the IPv6 address of source interface for the SNMP trap.
<VRF-NAME>	Specifies the name of a VRF associated to the source interface for the SNMP trap.

Examples

Configuring SNMP trap source interface for a VRF.


```
switch(config)# snmp-server trap-source interface 1/1/12 vrf sample
switch(config)# snmp-server trap-source interface loopback10 vrf sample
switch(config)# snmp-server trap-source interface vlan23 vrf sample
```

Configuring SNMP trap source IP address for a VRF.

```
switch(config)# snmp-server trap-source 10.0.0.1 vrf red
switch(config)# snmp-server trap-source 1001::1 vrf red
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server trap vsx

```
snmp-server trap vsx
no snmp-server trap vsx
```

Description

Enables sending the SNMP traps for VSX related events. VSX trap generation is disabled by default. The **no** form of this command disables sending the SNMP traps for VSX related events. The trap support is available for the following VSX events:

- ISL up and down
- KA up and down
- MCLAG up and down

Parameter	Description
vsx	Specifies SNMP traps for VSX events.

Examples

Enabling the VSX traps:

```
switch(config)# snmp-server trap vsx
```

```
switch(config)# show vsx configuration trap
SNMP traps : Enabled
```

Disabling the VSX traps:

```
switch(config)# no snmp-server trap vsx
```

```
switch(config)# show vsx configuration trap
SNMP traps : Disabled
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server view

```
snmp-server view <VIEWNAME> <OID_TREE> [<MASK>] <included/excluded>
no snmp-server view <VIEWNAME> <OID_TREE> [<MASK>] <included/excluded>
```

Description

Configures an SNMP MIB view.

The **no** form of this command removes the specified SNMP MIB view.

Parameter	Description
<VIEWNAME>	Specifies the name of the SNMP MIB view. Supports up to a maximum of 32 characters.
<OID_TREE>	Specifies the OID tree to be included or excluded in SNMP MIB view.
<MASK>	Specifies the OID mask value. The values must be in hexadecimal character separated with : (colon).
<included/excluded>	Specifies the OID tree that is included in or excluded from the SNMP MIB view.

Usage

You can configure a maximum of 50 SNMP MIB views. The following VTY message is displayed when the configuration exceeds the maximum SNMP MIB views:

```
switch(config)# snmp-server view name51 1.3.6.1.2.1.1 fe:00 included
Configuration failed: Maximum allowed views are configured.
```

Examples

Configuring the SNMP MIB views:

```
switch(config)# snmp-server view name1 .1.3.6.1.2.1.2.2.1.1.1 FF:A0 included
switch(config)# snmp-server view name2 IF-MIB::ifindex included
switch(config)# snmp-server view name4 1.3.6.1.2.1.1 fe:00 included
```

Removing an SNMP MIB view:

```
switch(config)# no snmp-server view name4 1.3.6.1.2.1.1 fe:00 included
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmp-server vrf

```
snmp-server vrf <VRF-NAME>
no snmp-server vrf <VRF-NAME>
```

Description

Configures a VRF on which the SNMP agent listens for incoming requests. By default, the SNMP agent does not listen on any VRF. 4100i, 6000, and 6100 only support default VRF. **The SNMP agent can listen on multiple VRFs.**

The **no** form of this command stops the SNMP agent from listening for incoming requests on the specified VRF.

Parameter	Description
<VRF-NAME>	Specifies the name of a VRF.

Examples

Configuring the SNMP agent to listen on VRF **default**.

```
switch(config)# snmp-server vrf default
```

Configuring the SNMP agent to listen on VRF **mgmt**.

```
switch(config)# snmp-server vrf mgmt
```

Configuring the SNMP agent to listen on used-defined VRF **myvrf**.

```
switch(config)# snmp-server vrf myvrf
```

Stopping the SNMP agent from listening on VRF **default**.

```
switch(config)# no snmp-server vrf default
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmpv3 context

```
snmpv3 context <NAME> vrf <VRF-NAME> [community <STRING>]  
no snmpv3 context <NAME> [vrf <VRF-NAME>] [community <STRING>]
```

Description

Creates an SNMPv3 context on the specified VRF.

The **no** form of this command removes the specified SNMP context.

Parameter	Description
<NAME>	Specifies the name of the context. Range: 1 to 32 printable ASCII characters, excluding space and question mark (?).

Parameter	Description
<code>vrf <VRF-NAME></code>	Specifies the VRF associated with the context. Default: default.
<code>community <STRING></code>	Specifies the SNMP community string associated with the context. Range: 1 to 32 printable ASCII characters, excluding space and question mark. Default: public.

Examples

Creating an SNMPv3 context named **newContext**:

```
switch(config)# snmpv3 context newContext
```

Creating an SNMPv3 context named **newContext** on VRF **myVrf** and with community string **private**.

```
switch(config)# snmpv3 context newContext vrf myVrf community private
```

Removing the SNMPv3 context named **newContext** on VRF **myVrf**:

```
switch(config)# no snmpv3 context newContext vrf myVrf
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

snmpv3 engine-id

```
snmpv3 engine-id <ENGINE-ID>
no snmpv3 engine-id <ENGINE-ID>
```

Description

Configures the SNMPv3 SNMP engine-id allowing an administrator to configure a unique SNMP engine-id for the switch. This engine-id is used by the NMS management tool to identify and distinguish multiple switches on the same network.

The **no** form of this command restores the default engine-id, created by the switch using a combination of the enterprise OID value and the switch's mac address.

Parameter	Description
<ENGINE-ID>	SNMPv3 SNMP engine-id in colon separated hexadecimal notation.

Examples

Configuring the SNMPv3 engine-id:

```
switch(config)#
switch(config)# snmpv3 engine-id
WORD SNMPv3 snmp engine-id in colon seperated hexadecimal notation
switch(config)# snmpv3 engine-id 01:23:45:67:89:ab:cd:ef:01:23:45:67
```

Restoring the default SNMPv3 engine-id:

```
switch(config)# no snmpv3 engine-id
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmpv3 security-level

```
snmpv3 security-level {auth | auth-privacy}
no snmpv3 security-level {auth | auth-privacy}
```

Description

Configures the SNMPv3 security level. The security level determines which SMNPv3 users defined by the command `snmpv3 user` are able to connect.

The **no** form of this command changes the security level as follows:

- **no snmpv3 security-level auth:** Sets the security level to **auth-privacy**.
- **no snmpv3 security-level auth-privacy:** Sets the security level to no authentication or privacy, allowing any SNMP user to connect.

Parameter	Description
auth	SNMPv3 users that support authentication, or authentication and privacy are allowed.
auth-privacy	Only SNMPv3 users with both authentication and privacy are allowed. This is the highest level of SNMPv3 security. Default.

Examples

Setting the SNMPv3 security level to authentication and privacy:

```
switch(config)# snmpv3 security-level auth-privacy
```

Setting the SNMPv3 security level to authentication only:

```
switch(config)# snmpv3 security-level auth
```

Setting the SNMPv3 security level to no authentication and no privacy:

```
switch(config)# no snmpv3 security-level auth-privacy
```

Restoring the default SNMPv3 security level to authentication and privacy:

```
switch(config)# no snmpv3 security-level auth
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmpv3 user

```
snmpv3 user <NAME>
    [auth <AUTH-PROTO> auth-pass [{plaintext | ciphertext} <AUTH-PASS>]]
    [priv <PRIV-PROTO> priv-pass [{plaintext | ciphertext} <PRIV-PASS>]]
    [access-level ro|rw]
```

```
no snmpv3 user <NAME>
```

```
[auth <AUTH-PROTO> auth-pass [{plaintext | ciphertext} <AUTH-PASS>]]
[priv <PRIV-PROTO> priv-pass [{plaintext | ciphertext} <PRIV-PASS>]]
[access-level ro|rw]
```

Description

Creates an SNMPv3 user and adds it to an SNMPv3 context. The SNMPv3 security level (set with command **snmpv3 security-level**) determines which users are allowed to authenticate.

The **no** form of this command removes the specified SNMPv3 user.



When updating the authentication protocols and privacy protocols for the existing SNMPv3 users, you must also update the access level. Otherwise, the access level will be set to read-only.

Parameter	Description
<NAME>	Specifies the SNMPv3 username. Range 1 to 32 printable ASCII characters, excluding space and question mark (?).
access-level	Configures the access level for the SNMPv3 user: ▪ ro: Allow read-only access for the SNMPv3 user ▪ rw: Allow read-write access for the SNMPv3 user
auth <AUTH-PROTO>	Sets the authentication protocol used to validate user logins. Supported protocols are md5 , sha , sha224 , sha256 , sha384 , and sha512 .
auth-pass [{plaintext ciphertext} <AUTH-PASS>]	Specifies the SNMPv3 user authentication password. Range for plaintext is 8 to 32 printable ASCII characters, excluding space and question mark (?). Range for ciphertext is 1 to 256 printable ASCII characters. Ciphertext is used when copying user configuration settings between switches. NOTE: Authentication passwords that include special characters must be enclosed in single quotation marks ('). For example, 'auth-pwd20246!@#'.
priv <PRIV-PROTO>	Sets the SNMPv3 privacy protocol (encryption method). Supported privacy protocols are aes , aes192 , aes256 , and des .
priv-pass [{plaintext ciphertext} <PRIV-PASS>]	Specifies the SNMPv3 user privacy encryption password. Range for plaintext is 8 to 32 printable ASCII characters, excluding space and question mark (?). Range for ciphertext is 1 to 256 printable ASCII characters. Ciphertext is used when copying user configuration settings between switches.

Parameter	Description
	NOTE: Authentication passwords that include special characters must be enclosed in single quotation marks ('). For example, 'priv-pwd20246!@#'.



When the authentication password is not provided on the command line, plaintext authentication password prompting occurs upon pressing Enter, followed by privacy encryption protocol prompting, and finally plaintext encryption password prompting. The entered password characters are masked with asterisks.



When the authentication type and password plus the privacy protocol (encryption method) are provided on the command line but the encryption password is not provided, plaintext encryption password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Defining SNMPv3 user **Admin1** using **sha** authentication and **des** privacy encryption with provided plaintext passwords:

```
switch(config)# snmpv3 user Admin1 auth sha auth-pass plaintext F82#450h
priv des priv-pass plaintext F82#4eva
```

Defining SNMPv3 user **Admin2** using **MD5** authentication and **AES** privacy encryption with provided authentication password and privacy encryption type but prompted encryption password:

```
switch(config)# snmpv3 user Admin2 auth md5 auth-pass plaintext F82#450h
priv aes priv-pass
Enter the privacy encryption key: *****
Re-Enter the privacy encryption key: *****
```

Defining SNMPv3 user **Admin2** using **MD5** authentication and **AES** privacy encryption with plaintext password prompting and privacy encryption selection:

```
switch(config)# snmpv3 user Admin2 auth md5 auth-pass
Enter the authentication password: *****
Re-Enter the authentication password: *****

Configure the privacy protocol (y/n)? y
Enter the privacy protocol (aes/des)? aes

Enter the privacy encryption key: *****
Re-Enter the privacy encryption key: *****
```

Removing SNMPv3 user **Admin1**:

```
switch(config)# no snmpv3 user Admin1
```

Creating an SNMP user on switch 1 and then creating the same user on switch 2 by copying from the switch 1 configuration:

On switch 1, configure a user named **Admin3**, and then use the **show running-config** command to display switch configuration. Save a copy of the full **snmpv3 user** command (shown by **show running-config**). This saved command is used on switch 2.

```
switch1(config)# snmpv3 user Admin3 auth sha auth-pass plaintext F82#450h
                  priv des priv-pass plaintext F82#4eva
switch1(config)# exit
switch1# show running-config
Current configuration:
!
!Version AOS-CX xx.xx.xx.xxxxxx
!
snmpv3 user Admin3 auth sha auth-pass ciphertext AQBaf2d...FJVcZ3o=
priv des priv-pass ciphertext AQBaH2p...2jfTFwQ=
ssh server vrf mgmt
!
interface mgmt
    no shutdown
    ip dhcp
    vlan 1
```

On switch 2, execute the **snmpv3 user** command that you saved from switch 1 (as shown by **show running-config**). This creates the user on switch 2 with the same configuration.

```
switch2(config)# snmpv3 user Admin3 auth sha auth-pass ciphertext
AQBaf2d...FJVcZ3o=
                  priv des priv-pass ciphertext AQBaH2p...2jfTFwQ=
```

The following command sets a read-write access level for an SNMPv3 user with the user name **user1**.

```
switch(config)# snmpv3 user user1 auth md5 auth-pass plaintext abc1234 access-
level rw
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.13	Following authentication protocols are supported: sha224 , sha256 , sha384 , and sha512 . Following privacy protocols are supported: aes192 and aes256 .
10.09	The access-level parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

snmpv3 user view

```
snmpv3 user <USER-NAME> view <VIEW-NAME>
no snmpv3 user <USER-NAME> view <VIEW-NAME>
```

Description

Associates a user with an existing SNMP MIB view.

The **no** form of this command removes the associated user from the specified SNMP MIB view.

Parameter	Description
<USER-NAME>	Specifies the user name for the SNMP MIB view. Accepts a maximum of 32 characters.
<VIEWNAME>	Specifies the view name for the SNMP MIB view. Accepts a maximum of 32 characters.

Examples

Adding a user in the existing SNMP MIB view:

```
switch(config)# snmpv3 user nw-admin view my-nw-view
```

Removing the user from the SNMP MIB view:

```
switch(config)# no snmpv3 user nw-admin view my-nw-view
```

Attaching unconfigured or unknown SNMP view to an SNMPv3 user:

```
switch(config)# snmpv3 user nw-admin view myView
View myView is not configured.
```



For more information on features that use this command, refer to the SNMP/MIB Guide for your switch model.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

Source-interface selection commands

ip source-interface

```
ip source-interface <PROTOCOL> {<IP-ADDR>|interface <IFNAME>} [vrf <VRF-NAME>]
no ip source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]
```

Description

Configures the IPv4 source-interface interface to use for the specified protocol. If a VRF is not given, the default VRF applies.

The **no** form of this command removes the specified configuration.

Parameter	Description
<PROTOCOL>	Specifies the protocol to configure. ▪ all: Selects the source for all protocols covered by this command. ▪ central: Selects HPE Aruba Networking Central. ▪ dhcp_relay: Selects DHCP relay. When you configure a dhcp_relay source interface, you must also enable DHCP relay Option 82 using the dhcp-relay option 82 source-interface command. ▪ dns: Selects DNS. ▪ http: Selects HTTP. ▪ ntp: Selects NTP. ▪ radius: Selects RADIUS. ▪ sflow: Selects sFlow. ▪ sftp-scp: Selects SFTP and SCP. ▪ ssh-client: Selects SSH Client. ▪ syslog: Selects the source for syslog packets. ▪ tacacs: Selects the source for TACACS packets. ▪ tftp: Selects TFTP.
<IFNAME>	Specifies the interface name.
<IP-ADDR>	Specifies the IPv4 address.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Configuring IPv4 source-interface interface 1/1/1 to use for the TFTP protocol:

```
switch(config)# ip source-interface tftp interface 1/1/1
```

Configuring IPv4 source-interface interface 1/1/2 to use for the TFTP protocol on VRF **green**:

```
switch(config)# ip source-interface tftp interface 1/1/2 vrf green
```

Removing IPv4 source-interface 1/1/1 configuration for the TFTP protocol:

```
switch(config)# no ip source-interface tftp interface 1/1/1
```

Removing source-interface interface 1/1/2 configuration for TFTP protocol on VRF **green**:

```
switch(config)# no ip source-interface tftp interface 1/1/2 vrf green
```

Configuring source-interface IPv4 10.1.1.1 to use for the TFTP protocol:

```
switch(config)# ip source-interface tftp 10.1.1.1
```

Configuring source-interface IPv4 10.1.1.2 to use for the TFTP protocol on VRF **green**:

```
switch(config)# ip source-interface tftp 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1 configuration for the TFTP protocol:

```
switch(config)# no ip source-interface tftp 10.1.1.1
```

Removing source-interface IPv4 10.1.1.2 configuration for TFTP protocol on VRF **green**:

```
switch(config)# no ip source-interface tftp 10.1.1.2 vrf green
```

Configuring source-interface IPv4 10.1.1.1 to use for the DNS protocol:

```
switch(config)# ip source-interface dns 10.1.1.1
```

Configuring source-interface IPv4 10.1.1.2 to use for the DNS protocol on VRF **green**:

```
switch(config)# ip source-interface dns 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1 configuration for the DNS protocol:

```
switch(config)# no ip source-interface tftp 10.1.1.1
```

Removing source-interface IPv4 10.1.1.2 configuration for the DNS protocol on VRF **green**:

```
switch(config)# no ip source-interface dns 10.1.1.2 vrf green
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.12.1000	Added central , sftp-scp , and ssh-client parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ipv6 source-interface <protocol>

```
ipv6 source-interface <PROTOCOL> {<IPV6-ADDR>|interface <IFNAME>} [vrf <VRF-NAME>]  
no ipv6 source-interface <PROTOCOL> {<IPV6-ADDR>|interface <IFNAME>} [vrf <VRF-NAME>]
```

Description

Configures the IPv6 source-interface interface to use for the specified protocol. If a VRF is not given, the default VRF applies.

The **no** form of this command removes all configurations.

Parameter	Description
<PROTOCOL>	Specifies the protocol to configure. ▪ all: Selects the source for all protocols covered by this command. ▪ central: Selects HPE Aruba Networking Central. ▪ dhcp_relay: Selects DHCP relay. When you configure a dhcp_relay source interface, you must also enable DHCP relay Option 82 using the dhcp-relay option 82source-interface command. ▪ dns: Selects DNS. ▪ http: Selects HTTP. ▪ ntp: Selects NTP. ▪ radius: Selects RADIUS. ▪ sflow: Selects sFlow. ▪ sftp-scp: Selects SFTP and SCP. ▪ ssh-client: Selects SSH Client. ▪ syslog: Selects the source for syslog packets. ▪ tacacs: Selects the source for TACACS packets. ▪ tftp: Selects TFTP.

Parameter	Description
<IPv6-ADDR>	Specifies the IPv6 address.
<IFNAME>	Specifies the interface name.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Configuring IPv6 source-interface interface 1/1/1 to use for the TFTP protocol :

```
switch(config)# ipv6 source-interface tftp interface 1/1/1
```

Configuring IPv6 source-interface interface 1/1/2 to use for the TFTP protocol on VRF **green**:

```
switch(config)# ipv6 source-interface tftp interface 1/1/2 vrf green
```

Removing IPv6 source-interface interface 1/1/1 configuration for the TFTP protocol:

```
switch(config)# no ipv6 source-interface tftp interface 1/1/1
```

Removing IPv6 source-interface interface 1/1/2 configuration for the TFTP protocol on VRF **green**:

```
switch(config)# no ipv6 source-interface tftp interface 1/1/2 vrf green
```

Configuring source-interface IPv6 1111:2222 to use for the TFTP protocol:

```
switch(config)# ipv6 source-interface tftp 1111:2222
```

Configuring source-interface IPv6 1111:3333 to use for TFTP protocol on VRF **green**:

```
switch(config)# ipv6 source-interface tftp 1111:3333 vrf green
```

Removing source-interface IPv6 1111:2222 configuration for TFTP protocol:

```
switch(config)# no ipv6 source-interface tftp 1111:2222
```

Removing source-interface IPv6 1111:3333 configuration for TFTP protocol on VRF **green**:

```
switch(config)# no ipv6 source-interface tftp 1111:3333 vrf green
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.13.0001	Added the dns protocol parameter.
10.12.1000	Added central , sftp-scp , dhcp_relay and ssh-client parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ipv6 source-interface dns

```
ipv6 source-interface {dns | all} {interface | X:X::X:X} [vrf <VRF-NAME>]
[no] ipv6 source-interface {dns | all} {interface | X:X::X:X} [vrf <VRF-NAME>]
```

Description

Configures the IPv6 source-interface or source IP for IPv6 DNS clients.

The **no** form of this command removes all configurations.

Parameter	Description
<IPv6-ADDR>	Specifies the IPv6 address.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Configuring IPv6 source-interface DNS on 1::1:

```
switch(config)# ipv6 source-interface dns 1::1
vrf VRF Configuration
```

Configuring IPv6 source-interface DNS on 1::1 vrf **red**

```
switch(config)# ipv6 source-interface dns 1::1 vrf red
switch(config)# ipv6 source-interface dns interface vlan10
vrf VRF Configuration
```

Configuring IPv6 source-interface DNS on VLAN 10 and vrf **red**:

```
switch(config)# ipv6 source-interface dns interface vlan10 vrf red
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show ip source-interface

```
show ip source-interface <PROTOCOL> [vrf <VRF-NAME> | all-vrfs]
```

Description

Displays the source interface information for all VRFs or a specific VRF.

If a VRF is not specified, the default is displayed.

Parameter	Description
<code><PROTOCOL></code>	Specifies the protocol to show. <code>all</code> Shows the source interface configuration for all other protocols. <code>central</code> Shows the source interface configuration for HPE Aruba Networking Central. <code>dhcp relay</code> Shows the source interface configuration for DHCP relay. <code>dns</code> Shows the source interface configuration for DNS. <code>http</code> Shows the source interface configuration for HTTP. <code>ntp</code> Shows the source interface configuration for NTP. <code>radius</code> Shows the source interface configuration for radius. <code>sflow</code> Shows the source interface configuration for sFlow. <code>sftp-scp</code> Shows source interface configuration for SFTP and SCP.

Parameter	Description
<code>ssh-client</code>	Shows source interface configuration for SSH Client.
<code>syslog</code>	Shows the source interface configuration for syslog.
<code>tacacs</code>	Shows the source interface configuration for TACACS.
<code>tftp</code>	Shows the source interface configuration for TFTP.
<code>vrf <VRF-NAME></code>	Specifies the VRF name.
<code>all-vrfs</code>	Shows the source interface configuration for all VRFs.

Examples

Displaying all source-interface protocol configurations for VRF red:

```
switch# show ip source-interface all vrf red
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP      VRF
-----
all           1/1/1              red
switch#
```

Displaying all source-interface protocol configurations for default VRF:

```
switch# show ip source-interface all
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP      VRF
-----
all           1.1.1.1            default
switch#
```

Displaying all source-interface protocol configurations for all VRFs:

```
switch# show ip source-interface all all-vrfs
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP      VRF
-----
all           2.2.2.2            all-vrfs
all           1.1.1.1            default
all           1/1/1/1            red
switch#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.12.1000	Added <code>central</code> , <code>sftp-scp</code> , and <code>ssh-client</code> parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ipv6 source-interface

```
show ipv6 source-interface <PROTOCOL> [detail] [vrf <VRF-NAME> | all-vrfs]
```

Description

Displays the IPV6 source interface information configured in the router for all VRFs or a specific VRF. If a VRF is not specified, the default is displayed.

Parameter	Description
<code><PROTOCOL></code>	Specifies the protocol to show. <code>all</code> Shows the source interface configuration for all other protocols. <code>central</code> Shows the source interface configuration for HPE Aruba Networking Central. <code>dhcp_relay</code> Shows the source interface configuration for DHCP really. <code>dns</code> Shows the source interface configuration for DNS. <code>http</code> Shows the source interface configuration for HTTP. <code>ntp</code> Shows the source interface configuration for NTP. <code>radius</code> Shows the source interface configuration for radius. <code>sflow</code> Shows the source interface configuration for sFlow. <code>sftp-scp</code> Shows source interface configuration for SFTP and SCP. <code>ssh-client</code> Shows source interface configuration for SSH Client. <code>syslog</code> Shows the source interface configuration for syslog.

Parameter	Description
	tacacs Shows the source interface configuration for TACACS.
	tftp Shows the source interface configuration for TFTP.
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Shows the source interface configuration for all VRF.

Examples

Displaying all IPv6 source-interface protocol configurations for the **default** VRF:

```
switch# show ipv6 source-interface all
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP              VRF
-----
all           1111::2222         default
switch#
```

Displaying all IPv6 source-interface protocol configuration for VRF red:

```
switch# show ipv6 source-interface all vrf red
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP              VRF
-----
all           1/1/1             2005::2             red
switch#
```

Displaying all IPv6 source-interface protocol configurations for all VRFs:

```
switch# show ipv6 source-interface all all-vrfs
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP              VRF
-----
all           2222::3333         all-vrfs
all           1111::2222         default
all           1/1/1             2::2               red
switch#
```

Displaying all IPv6 source-interface protocol configurations for dns all VRFs:

```
switch# show ipv6 source-interface dns all-vrfs
Source-interface Configuration Information
-----
--
Protocol      Src-Interface      Src-IP              VRF
-----
--
dns           1::3              blue
switch#
```

dns	1::4	default
dns	1::2	red



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.13	Added the <code>dns</code> protocol parameter.
10.12.1000	Added <code>central</code> , <code>sftp-scp</code> , and <code>ssh-client</code> parameters.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show running-config

show running-config

Description

Displays the current running configuration.

Examples

Displaying the running configuration (only items of interest to source interface selection are shown in this example output command):



HPE Aruba Networking Central is the priority agent. If no command is specified for ip source-interface, Central will choose the command automatically if it is reachable on any of the known ports.

```
switch# show running-config
vrf green
ip source-interface tftp interface 1/1/2 vrf green
ip source-interface radius interface 1/1/2 vrf green
ip source-interface ntp interface 1/1/2 vrf green
ip source-interface tacacs interface 1/1/2 vrf green
ip source-interface dns interface 1/1/2 vrf green
ip source-interface ubt interface 1/1/2 vrf green
ip source-interface central interface 1/1/2 vrf green
ip source-interface all interface 1/1/2 vrf green
ipv6 source-interface tftp 2222::3333 vrf green
ipv6 source-interface radius 2222::3333 vrf green
```

```

ipv6 source-interface ntp 2222::3333 vrf green
ipv6 source-interface tacacs 2222::3333 vrf green
ipv6 source-interface ubt 2222::3333 vrf green
ipv6 source-interface central 2222::3333 vrf green
ipv6 source-interface all 2222::3333 vrf green
ip source-interface tftp 10.20.3.1
ip source-interface radius 10.20.3.1
ip source-interface ntp 10.20.3.1
ip source-interface tacacs 10.20.3.1
ip source-interface psm 10.20.3.1
ip source-interface workload_migration 10.20.3.1
ip source-interface erspan 10.20.3.1
ip source-interface ipfix 10.20.3.1
ip source-interface dns 10.20.3.1
ip source-interface ubt 10.20.3.1
ip source-interface central 10.20.3.1
ip source-interface all 10.20.3.1
interface 1/1/1
    no shutdown
    ip address 10.20.3.1/24
interface 1/1/2
    vrf attach greendefault
    ip address 20.1.1.1/24
    ipv6 address 2222::3333/64
interface 1/1/45
    no shutdown
    ip address 100.1.0.1/24
    ipv6 address 1111::2222/64
ip route 100.2.0.0/24 10.20.3.2
switch#

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

SSH client commands

ssh (client login)

```
ssh [<USERNAME>@]{<IPv4> | <HOSTNAME>} [vrf <VRF-NAME>] [port <PORT-NUMBER>]
```

Description

Establishes a client session with an SSH server which is typically another switch. username, vrf and port number are optional parameters. If a source ip address or source interface is configured for the ssh client protocol, the configuration values are used for establishing the client session with the SSH server.



The source interface can be configured using the IP source interface configuration commands described in the Fundamentals Guide.

Parameter	Description
<USERNAME>	Specifies the username that the client uses to log in to an SSH server. When omitted, the username of the current session is used.
<IPv4>	Specifies the SSH server to which the SSH client will connect as an IPv4 address.
<HOSTNAME>	Specifies the SSH server to which the SSH client will connect as a host name.
vrf <VRF-NAME>	Specifies the VRF to be used for the SSH client session. When omitted, the default VRF named <code>default</code> is used.
port <PORT-NUMBER>	Specifies the SSH server TCP port number. When omitted, the default TCP port 22 is used.

Examples

Establishing an SSH client session (using the management VRF) with an SSH server:

```
switch# ssh admin@10.0.11.180 vrf mgmt
```

Establishing an SSH client session (using the default VRF and a specific port) with an SSH server:

```
switch# ssh admin@10.0.11.175 port 223
```

Configuring a test user on switch 1 and then connecting to switch 1 from switch 2 using the SSH client on the mgmt VRF:


```
** Configuring a test user on switch 1 **  
switch(config)# user-group test  
switch(config-usr-grp-test)# permit cli command ".*"  
switch(config)# exit  
switch(config)# user test-user group test password plaintext tst#9J  
  
** On switch 2, connecting to switch 1 using the SSH client **  
switch# ssh test-user@10.0.11.177 vrf mgmt
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

ssh (client login)

ssh [*<USERNAME>*@]{*<IPV4>* | *<HOSTNAME>*} [*vrf <VRF-NAME>*] [*port <PORT-NUMBER>*]

Description

Establishes a client session with an SSH server which is typically another switch. username, vrf and port number are optional parameters. If a source ip address or source interface is configured for the ssh client protocol, the configuration values are used for establishing the client session with the SSH server.



The source interface can be configured using the IP source interface configuration commands described in the Fundamentals Guide.

Parameter	Description
<i><USERNAME></i>	Specifies the username that the client uses to log in to an SSH server. When omitted, the username of the current session is used.
<i><IPV4></i>	Specifies the SSH server to which the SSH client will connect as an IPv4 address.
<i><HOSTNAME></i>	Specifies the SSH server to which the SSH client will connect as a host name.
<i>vrf <VRF-NAME></i>	Specifies the VRF to be used for the SSH client session. When omitted, the default VRF named <code>default</code> is used.
<i>port <PORT-NUMBER></i>	Specifies the SSH server TCP port number. When omitted, the default TCP port 22 is used.

Examples

Establishing an SSH client session (using the management VRF) with an SSH server:

```
switch# ssh admin@10.0.11.180 vrf mgmt
```

Establishing an SSH client session (using the default VRF and a specific port) with an SSH server:

```
switch# ssh admin@10.0.11.175 port 223
```

Configuring a test user on switch 1 and then connecting to switch 1 from switch 2 using the SSH client on the mgmt VRF:

```
** Configuring a test user on switch 1 **
switch(config)# user-group test
switch(config-usr-grp-test)# permit cli command ".*"
switch(config)# exit
switch(config)# user test-user group test password plaintext tst#9J

** On switch 2, connecting to switch 1 using the SSH client **
switch# ssh test-user@10.0.11.177 vrf mgmt
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

erase ssh sftp-server

```
erase ssh sftp-server {recursive} FILENAME
```

Description

Deletes a specified file or directory within the SFTP server local storage directory. All filenames are interpreted relative to the SFTP server local storage directory.

Parameter	Description
recursive	Recursively delete a directory.
FILENAME	

Examples

Deleting a specified filename:

```
switch# erase ssh sftp-server filename
```

Deleting a specified directory:

```
switch# erase ssh sftp-server recursive /path/to/dir1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ssh server

```
show ssh server [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

Description

Shows the SSH server configuration for the specified VRF. Administrators can show the server configuration of all VRFs by using the **all-vrfs** parameter. If no VRF name is provided in this command, the command shows the SSH server configuration on the default VRF.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Selects all VRFs.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the SSH server configuration on the default VRF:

```
switch# show ssh server
```

```
SSH server configuration on VRF default :
IP Version      :   IPv4 and IPv6      SSH Version      :   2.0
TCP Port        :   22                  Grace Timeout (sec) :   60
Max Auth Attempts :   6                  Server Status      :   running
Allow-list      :   disabled
Ciphers:
chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:
curve25519-sha256, curve25519-sha256@libssh.org,
ecdh-sha2-nistp256,ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,
diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,
diffie-hellman-group14-sha1

MACs:
hmac-sha1-etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256,hmac-sha2-512,hmac-sha1

Public Key Algorithms:
rsa-sha2-256, rsa-sha2-512ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,
x509v3-ecdsa-sha2-nistp521
```

Showing the SSH server configuration on the management VRF:

```
switch# show ssh server vrf mgmt
```

SSH server configuration on VRF mgmt :

IP Version	: IPv4 and IPv6	SSH Version	: 2.0
TCP Port	: 22	Grace Timeout (sec)	: 120
Max Auth Attempts	: 6		

Allow-list: disabled

Ciphers:

chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:

ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:

curve25519-sha256, curve25519-sha256@libssh.org,
ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521,
diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512,
diffie-hellman-group18-sha512, diffie-hellman-group14-sha256,
diffie-hellman-group14-sha1

MACs:

hmac-sha1-etm@openssh.com, umac-64@openssh.com,
umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1

Public Key Algorithms:

rsa-sha2-256, rsa-sha2-512, ssh-rsa, ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,

Showing the SSH server configuration for all VRFs:

```
switch# show ssh server all-vrfs
```

SSH server configuration on VRF default :

IP Version	: IPv4 and IPv6	SSH Version	: 2.0
TCP Port	: 22	Grace Timeout (sec)	: 120
Max Auth Attempts	: 6		

Ciphers:

chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc

Host Key Algorithms:

ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa

Key Exchange Algorithms:

```
curve25519-sha256, curve25519-sha256@libssh.org,  
ecdh-sha2-nistp256,ecdh-sha2-nistp384, ecdh-sha2-nistp521,  
diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,  
diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,
```

MACs:

```
hmac-sha1-etm@openssh.com, umac-64@openssh.com,  
umac-128@openssh.com, hmac-sha2-256,hmac-sha2-512,hmac-sha1
```

Public Key Algorithms:

```
rsa-sha2-256, rsa-sha2-512ssh-rsa, ecdsa-sha2-nistp256,  
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,  
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,  
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,  
x509v3-ecdsa-sha2-nistp521
```

SSH server configuration on VRF mgmt :

IP Version	: IPv4 and IPv6	SSH Version	: 2.0
TCP Port	: 22	Grace Timeout (sec)	: 120
Max Auth Attempts	: 6		

Ciphers:

```
chacha20-poly1305@openssh.com, aes128-ctr, aes192-cbc,  
aes128-cbc, aes192-ctr, aes256-gcm@openssh.com,  
aes128-gcm@openssh.com, aes256-ctr, aes256-cbc
```

Host Key Algorithms:

```
ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,  
ssh-ed25519, rsa-sha2-256, rsa-sha2-512, ssh-rsa
```

Key Exchange Algorithms:

```
curve25519-sha256, curve25519-sha256@libssh.org,  
ecdh-sha2-nistp256,ecdh-sha2-nistp384, ecdh-sha2-nistp521,  
diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,  
diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,  
diffie-hellman-group14-sha1
```

MACs:

```
hmac-sha1-etm@openssh.com, umac-64@openssh.com,  
umac-128@openssh.com, hmac-sha2-256,hmac-sha2-512,hmac-sha1
```

Public Key Algorithms:

```
rsa-sha2-256, rsa-sha2-512ssh-rsa, ecdsa-sha2-nistp256,  
ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519,  
x509v3-rsa2048-sha256, x509v3-ssh-rsa, x509v3-sign-rsa,  
x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384,
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ssh server sessions

```
show ssh server sessions [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

Description

Shows the active SSH sessions on a specified VRF or on all VRFs. If no VRF is specified, the active sessions on the **default** VRF are shown.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Selects all VRFs.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

If you provide the command with a VRF name, the command shows the active SSH session for the specified VRF. Any user can show sessions of all VRFs by using the **all-vrfs** parameter. The maximum number of sessions per VRF is five. The maximum SSH idle session timeout is 60 seconds.

Examples

Showing the active SSH sessions on the default VRF:

```
switch# show ssh server sessions

SSH sessions on VRF default
IPv4 SSH Sessions
  Server IP       : 10.1.1.1
  Client IP       : 10.1.1.2
  Client Port     : 58835

IPv6 SSH Sessions
  Server IP       : FF01:0:0:0:0:0:0:FB
  Client IP       : FF01:0:0:0:0:0:0:FC
  Client Port     : 58836
```

Showing the SSH server configuration for all VRFs:

```
switch# show ssh server sessions all-vrf

SSH sessions on VRF mgmt
IPv4 SSH Sessions
```



```

Server IP      : 10.1.1.1
Client IP     : 10.1.1.2
Client Port   : 58835

IPv6 SSH Sessions
Server IP     : FF01:0:0:0:0:0:0:FB
Client IP     : FF01:0:0:0:0:0:0:FC
Client Port   : 58836

SSH sessions on VRF default
IPv4 SSH Sessions
Server IP     : 20.1.1.1
Client IP     : 20.1.1.2
Client Port   : 58837

IPv6 SSH Sessions
Server IP     : FF01:0:0:0:0:0:0:FD
Client IP     : FF01:0:0:0:0:0:0:FE
Client Port   : 58838

```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ssh sftp-server usage

`show ssh sftp-server usage`

Description

Shows the amount of used storage space along with the total amount of allotted space.

Examples

Showing the amount of used storage and allotted space:

```

switch# show ssh sftp-server usage
Used:      4K
Allotted:  4096M

```

Copying files to and from the SFTP local storage directory:

```
switch# copy primary local:/image.swi
switch# copy local:/image.swi secondary
switch# copy running-config local:/config.txt cli
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

ssh ciphers

```
ssh ciphers <CIPHERS-LIST>
no ssh ciphers
```

Description

Configures SSH to use a set of ciphers in the specified priority order. Ciphers in SSH are used for privacy of data being transported over the connection. The first cipher type entered in the CLI is considered a first priority. Each option is an algorithm that is used to encrypt the link and each name indicates the algorithm and cryptographic parameters that are used. Only ciphers that are entered by the user are configured.

The **no** form of this command removes the configuration of ciphers and reverts SSH to use the default set of ciphers.

Parameter	Description
<CIPHERS-LIST>	Valid ciphers: ■ aes128-cbc ■ aes192-cbc ■ aes256-cbc ■ aes128-ctr ■ aes192-ctr ■ aes256-ctr ■ aes128-gcm@openssh.com ■ aes256-gcm@openssh.com ■ chacha20-poly1305@openssh.com Default set of ciphers in priority order (highest at top): ■ chacha20-1305@openssh.com

Parameter	Description
	▪ aes128-ctr ▪ aes192-ctr ▪ aes256-ctr ▪ aes128-gcm@openssh.com ▪ aes256-gcUm@openssh.com

Examples

Configuring SSH to use only specified ciphers in the priority order:

```
switch(config) # ssh ciphers chacha20-poly1305@openssh.com aes256-ctr aes256-cbc
```

Reverting SSH to use the default set of ciphers:

```
switch(config) # no ssh ciphers
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh host-key

```
ssh host-key {ecdsa [ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | ecdsa-sha2-nistp521] |
ed25519 | rsa [bits {2048 | 4096}] }
```

Description

Generates an SSH host-key pair.

Parameter	Description
ecdsa	Selects the ECDSA host-key pair type as ecdsa-sha2-nistp256 (the default), ecdsa-sha2-nistp384 , or ecdsa-sha2-nistp521 .
ed25519	Selects the ED25519 host-key pair.

Parameter	Description
rsa	Selects the RSA host-key pair. Optionally, the key bit length is selected with either bits 2048 (the default) or bits 4096 .

Usage

When an SSH server is enabled on a VRF for the first time, host-keys are generated.

If the host-key of the given type exists, a warning message is displayed with a request to overwrite the previous host-key with the new key.

Examples

Overwriting an old ECDSA host-key with a new ecdsa-sha2-nistp384 host-key:

```
switch(config)# ssh host-key ecdsa ecdsa-sha2-nistp384
ecdsa host-key will be overwritten.
Do you want to continue (y/n)?
```

Overwriting an old RSA host-key with a new RSA host-key with 2048 bits:

```
switch(config)# ssh host-key rsa bits 2048
rsa host-key will be overwritten.
Do you want to continue (y/n)?
```

Overwriting an ECDSA host-key with an ED25519 host-key pair:

```
switch(config)# ssh host-key ed25519
ed25519 host-key will be overwritten.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh host-key-algorithms

```
ssh host-key-algorithms <HOST-KEY-ALGORITHMS-LIST>
no ssh host-key-algorithms
```

Description

Configures SSH to use a set of host key algorithms in the specified priority order. Host key algorithms specify which host key types are allowed to be used for the SSH connection. The first host key entered in the CLI is considered a first priority. Each option represents a type of key that can be used. Host keys are used to verify the host that you are connecting to. This configuration allows you to control which host key types are presented to incoming clients, or which host key types to receive first from hosts. Only the host key algorithms that are specified by the user are configured.

The **no** form of this command removes the configuration of host key algorithms and reverts SSH to use the default set of algorithms.

Parameter	Description
<code><HOST-KEY-ALGORITHMS-LIST></code>	Default set of public key algorithms in priority order (highest at top), comprised of all possible valid algorithms: ▪ ecdsa-sha2-nistp256 ▪ ecdsa-sha2-nistp384 ▪ ecdsa-sha2-nistp521 ▪ ssh-ed25519 ▪ rsa-sha2-256 ▪ rsa-sha2-512 ▪ ssh-rsa

Examples

Configuring SSH to use only specified host key algorithms:

```
switch(config)# ssh host-key-algorithms ssh-rsa ssh-ed25519 ecdsa-sha2-nistp521
```

Reverting SSH to use the default set of host key algorithms:

```
switch(config)# no host-key-algorithms
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

ssh key-exchange-algorithms

```
ssh key-exchange-algorithms <KEY-EXCHANGE-ALGORITHMS-LIST>
no ssh key-exchange-algorithms
```

Description

Configures SSH to use a set of key exchange algorithm types in the specified priority order. The first key exchange type entered in the CLI is considered a first priority. Key exchange algorithms are used to exchange a shared session key with a peer securely. Each option represents an algorithm that is used to distribute a shared key in a way that prevents outside interference, manipulation, or recovery. Only the key exchange algorithms that are specified by the user are configured.

The **no** form of this command removes the configuration of key exchange algorithms and reverts SSH to use the default set of algorithms.

Parameter	Description
<code><KEY-EXCHANGE-ALGORITHMS-LIST></code>	Valid key exchange algorithms: ▪ curve25519-sha256 ▪ curve25519-sha256@libssh.org ▪ diffie-hellman-group-exchange-sha1 ▪ diffie-hellman-group-exchange-sha256 ▪ diffie-hellman-group14-sha1 ▪ diffie-hellman-group14-sha256 ▪ diffie-hellman-group16-sha512 ▪ diffie-hellman-group18-sha512 ▪ ecdh-sha2-nistp256 ▪ ecdh-sha2-nistp384 ▪ ecdh-sha2-nistp521 Default set of key exchange algorithms in priority order (highest at top): ▪ curve25519-sha256 ▪ curve25519-sha256@libssh.org ▪ ecdh-sha2-nistp256 ▪ ecdh-sha2-nistp384 ▪ ecdh-sha2-nistp521 ▪ diffie-hellman-group-exchange-sha256 ▪ diffie-hellman-group16-sha512 ▪ diffie-hellman-group18-sha512 ▪ diffie-hellman-group14-sha256 ▪ diffie-hellman-group-exchange-sha1

Examples

Configuring SSH to use a set of specified key exchange algorithms:

```
switch(config)# ssh key-exchange-algorithms ecdh-sha2-nistp256 curve25519-sha256
diffie-hellman-group-exchange-sha256
```

Reverting SSH to use the default set of key-exchange-algorithms:

```
switch(config)# no key-exchange-algorithms
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh known-host remove

```
ssh known-host remove {all | {<IPv4-ADDRESS> | <HOSTNAME> | <IPv6-ADDRESS>} }
```

Description

Clears the list of trusted SSH servers for your user account. When you download or upload a file to or from a server using SFTP, you establish a trusted SSH relationship with that server. Each user account maintains its own set of SSH server host-keys for every server to which the user previously connected.

Parameter	Description
all	Clears the trusted servers list.
<IPv4-ADDRESS>	Specifies the IPv4 address of the remote device.
<HOSTNAME>	Specifies the host name of the remote device. Range: up to 255 characters.
<IPv6-ADDRESS>	Specifies the IPv6 address of the remote device.

Examples

Clearing the trusted server list:

```
switch(config)# ssh known-host remove all
```

Removing a specified server from the trusted server list:

```
switch(config)# ssh known-host remove 1.1.1.1
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh macs

```
ssh macs <MACS-LIST>
no ssh macs
```

Description

Configures SSH to use a set of message authentication codes (MACs) in the specified priority order. The first MAC entered in the CLI is considered a first priority. MACs maintain the integrity of each message sent across an SSH connection. Each option represents an algorithm that can be used to provide integrity between peers. Only the MAC types that are specified by the user are configured.

The **no** form of this command removes the configuration of MACs and reverts SSH to use the default set of MACs.

Parameter	Description
<MACS-LIST>	Valid MACs: ▪ hmac-sha1 ▪ hmac-sha1-96 ▪ hmac-sha1-etm@openssh.com ▪ hmac-sha2-256 ▪ hmac-sha2-512 ▪ hmac-sha2-256-etm@openssh.com ▪ hmac-sha2-512-etm@openssh.com Default set of MACs in priority order (highest at top): ▪ hmac-sha2-256-etm@openssh.com ▪ hmac-sha2-512-etm@openssh.com ▪ hmac-sha1-etm@openssh.com ▪ hmac-sha2-256 ▪ hmac-sha2-512 ▪ hmac-sha1

Examples

Configuring SSH to use a set of specified MACs:

```
switch(config)# ssh macs hmac-sha2-256 hmac-sha2-512
```

Reverting SSH to use the default set of MACs:


```
switch(config)# no ssh macs
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh maximum-auth-attempts

```
ssh maximum-auth-attempts <ATTEMPTS>  
no maximum-auth-attempts
```

Description

Sets the SSH maximum number of authentication attempts.

The **no** form of the command resets the maximum to its default of 6.

Parameter	Description
<ATTEMPTS>	Specifies the maximum number of SSH authentication attempts. Range: 1 to 10. Default: 6.

Examples

Setting the maximum number of authentication attempts:

```
switch(config)# ssh maximum-auth-attempts 3
```

Resetting the maximum number of authentication attempts to its default of 6:

```
switch(config)# no maximum-auth-attempts
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh public-key-algorithms

```
ssh public-key-algorithms <PUBLIC-KEY-ALGORITHMS-LIST>
no ssh public-key-algorithms
```

Description

Configures SSH to use a set of public key algorithms in the specified priority order. The first public key type entered in the CLI is considered a first priority. Public key algorithms specify which public key types can be used for public key authentication in SSH. Each option represents a public key type that the SSH server can accept or that the SSH client can present to a server. Only the public key algorithms that are chosen by the user are configured.

The **no** form of this command removes the configuration of public key algorithms and reverts SSH to use the default set.

Parameter	Description
<PUBLIC-KEY-ALGORITHMS-LIST>	Default set of public key algorithms in priority order (highest at top), comprised of all possible valid algorithms: ▪ rsa-sha2-256 ▪ rsa-sha2-512 ▪ ssh-rsa ▪ ecdsa-sha2-nistp256 ▪ ecdsa-sha2-nistp384 ▪ ecdsa-sha2-nistp521 ▪ ssh-ed25519 ▪ x509v3-rsa2048-sha256 ▪ x509v3-ssh-rsa ▪ x509v3-sign-rsa ▪ x509v3-ecdsa-sha2-nistp256 ▪ x509v3-ecdsa-sha2-nistp384 ▪ x509v3-ecdsa-sha2-nistp521

Examples

Configuring SSH to use a set of specified public key algorithms:

```
switch(config)# ssh public-key-algorithms x509v3-ssh-rsa ssh-rsa rsa-sha2-256
```

Reverting SSH to use the default set of public key algorithms:

```
switch(config)# no ssh public-key-algorithms
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh server allow-list

```
ssh server allow-list
 ip <ipv4-addr>[mask]
 ipv6 <ipv6-addr>[mask]
 enable
 no
```

Description

Configure a list of addresses that will be the only hosts allowed to connect to the SSH servers running on all VRFs of the switch. By default, the allow-list is disabled and any host is allowed to connect given the correct authentication criteria. When the allow-list is enabled, only the hosts that fall under one of the entries may connect with the correct authentication criteria, all other hosts will be denied to attempt authentication.

Parameter	Description
<i>ip <ipv4-addr>[mask]</i>	An allowed host IP address and (optional) subnet in any of the following formats: ▪ A.B.C.D: An allowed IPv4 address ▪ A.B.C.D/M: An allowed IPv4 subnet with prefix length ▪ A.B.C.D W.X.Y.Z: An allowed IPv4 address with network mask ▪ A.B.C.D/W.X.Y.Z: An allowed IPv4 address with network mask
<i>ipv6 <iv6p-addr>[mask]</i>	An allowed host IPv6 address and (optional) subnet in any of the following formats: ▪ X:X::X:X: An allowed IPv6 address ▪ X:X::X:X/M: An allowed IPv6 subnet
enable	Enable the allow-list.
no ...	Negate a command or set its default.

Usage

The allow-list can contain up to 20 entries of IPv4 or IPv6 addresses, including entire subnets. The order in which the entries are added to the list does not matter. The configuration will only take effect once the allow-list is enabled by issuing the **enable** command in the *config-ssh-al* (**ssh server allow-list**) context.

When the allow-list is enabled, SSH servers on all VRFs will restart and all active SSH sessions will be terminated. The enabled allow-list may be modified to remove existing entries or add new entries, and each of those modifications will trigger an SSH server restart for all VRFs and will terminate all active SSH sessions, which may include the current user if they are connected via SSH. If you disable the allow-list before making changes and enabling the allow-list again once the changes are made, any host will be allowed to connect during the modification period before the allow-list is re-enabled. When the allow-list is disabled, the SSH servers on all VRFs will restart and active SSH sessions will persist.



Every SSH allow-list ends with an implicit **deny all** rule. When you add entries to an allow list, take care to avoid blocking connectivity to the SSH server. If an SSH allow-list is enabled with no entries configured, the **deny all** functionality will block all addresses, and the SSH server will be unusable.

Examples

Configuring and enabling an SSH server allow list

```
switch(config)# ssh server allow-list
switch(config-ssh-al)# 1.1.1.1
switch(config-ssh-al)# enable
Active SSH sessions will be terminated.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.12	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config and config-ssh-al contexts	Administrators or local user group members with execution rights for this command.

ssh server port

```
ssh server port <PORT-NUMBER>
no ssh server port [<PORT-NUMBER>]
```

Description

Configures SSH server to listen on a particular TCP port number. The default value is 22.

This port will be used for all VRFs that have SSH server enabled.



Configuring the TCP port number restarts the SSH server and terminates all active SSH sessions. It may take a few seconds for the SSH sessions to reach the running state on some VRFs.

The **no** form of the command resets the TCP port number to the default, 22.

Parameter	Description
<code><PORT-NUMBER></code>	Specifies the TCP port number. Range: 1 to 65535. Default: 22.

Examples

Configuring TCP port number 19222:

```
switch(config)# ssh server port 19222
```

Resetting the TCP port number to the default, 22:

```
switch(config)# no ssh server port
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.11.1000	Command introduced

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ssh server vrf

```
ssh server vrf <VRF-NAME>  
no ssh server vrf <VRF-NAME>
```

Description

Enables the SSH server on the specified VRF. SSH is disabled by default and will not be operational till the admin password is set on the switch. Note that the admin password is considered set even if it is configured to be empty.

The **no** form of the command disables the SSH server on the specified VRF. If no VRF is specified, by default the SSH server will be enabled on the **default** or **mgmt** VRF, depending on the switch model.

Parameter	Description
<code>vrf <VRF-NAME></code>	Specifies the VRF name.

Examples

Enabling the SSH server on the management VRF:

```
switch(config)# ssh server vrf mgmt
```

Disabling the SSH server on the management VRF:

```
switch(config)# no ssh server vrf mgmt
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	<code>config</code>	Administrators or local user group members with execution rights for this command.

ssh sftp-server

```
ssh sftp-server
no ssh sftp-server
```

Description

Enables the SFTP server on the switch, allowing secure file transfers. The SFTP server is disabled by default.

The **no** form of the command disables the SFTP server on the switch.

Parameter	Description
<code>vrf <VRF-NAME></code>	Specifies the VRF name.

Examples

Enabling the SFTP server on the switch:

```
switch(config)# ssh sftp-server
```

Disabling the SFTP server on the switch:

```
switch(config)# no ssh sftp-server
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
9300	config	Administrators or local user group members with execution rights for this command.

show ssh sftp-server file-system

```
show ssh sftp-server file-system
```

Description

List SFTP local storage directory.

Examples

Showing SFTP local storage directory:

```
switch# show ssh sftp-server file-system
total 16
drwxrwxr-x 4 admin administrators 4096 Jul 11 22:50 .
drwxr-xr-x 7 root root 4096 Jul 10 21:03 ..
drwxr-xr-x 2 admin administrators 4096 Jul 11 22:42 dir1
drwxr-xr-x 2 admin administrators 4096 Jul 11 22:42 dir2
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

show ssh sftp-server file-system

```
show ssh sftp-server file-system
```

Description

List SFTP local storage directory.

Examples

Showing SFTP local storage directory:

```
switch# show ssh sftp-server file-system
total 16
drwxrwxr-x 4 admin administrators 4096 Jul 11 22:50 .
drwxr-xr-x 7 root root 4096 Jul 10 21:03 ..
drwxr-xr-x 2 admin administrators 4096 Jul 11 22:42 dir1
drwxr-xr-x 2 admin administrators 4096 Jul 11 22:42 dir2
```



For more information on features that use this command, refer to the Security Guide for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

erase ssh sftp-server

```
erase ssh sftp-server {recursive} FILENAME
```

Description

Deletes a specified file or directory within the SFTP server local storage directory.

All filenames are interpreted relative to the SFTP server local storage directory.

Parameter	Description
recursive	Recursively delete a directory.

Parameter	Description
FILENAME	

Examples

Deleting a specified filename:

```
switch# erase ssh sftp-server filename
```

Deleting a specified directory:

```
switch# erase ssh sftp-server recursive /path/to/dir1
```



For more information on features that use this command, refer to the [Security Guide](#) for your switch model.

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Administrators or local user group members with execution rights for this command.

ip route

```
ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> |  
nullroute | reject]  
    {distance | name <WORD> | tag <VALUE> | track <WORD> | use-forwarding-address | vrf  
    <WORD>}]  
no ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> |  
nullroute | reject]  
    {distance | name <WORD> | tag <VALUE> | track <WORD> | use-forwarding-address | vrf  
    <WORD>}]  
  
ip route <DEST-IPV4-ADDR> <NETMASK> [<NEXTHOP-PORT-LAG-VLAN> | nullroute | reject]  
    {distance | name <WORD> | tag <VALUE> | vrf <WORD>}]  
no ip route <DEST-IPV4-ADDR> <NETMASK> [<NEXTHOP-PORT-LAG-VLAN> | nullroute | reject]  
    {distance | name <WORD> | tag <VALUE> | vrf <WORD>}]
```

Description

Adds an IPv4 static route on the default VRF.

The **no** form of this command deletes a IPv4 static route.



You can configure a maximum of 32 next hops per route.

Parameter	Description
<DEST-IPV4-ADDR>/<NETMASK>	Specifies the IPv4 route destination.
<NETMASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 32.
<NEXTHOP-ADDR>	Specifies the next hop address for reaching the destination in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<NEXTHOP-PORT-LAG-VLAN>	Specifies the next hop as an outgoing interface.
nullroute	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.
reject	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
distance <VALUE>	Specifies the administrative distance to associate with this static route. Range: 1 to 255. Default: 1.
name <WORD>	Specifies the name for the destination route. Range: 1 to 64 characters.

Parameter	Description
tag <VALUE>	Specifies and assigns tag for the route. Range: 1 to 4294967295.
track <WORD>	Specifies a name for the track object.
use-forwarding-address	Specifies the nexthop address as forwarding address.
vrf <WORD>	Specifies the VRF route leak destination.

Examples

```

switch(config)# ip route 10.0.0.0/24 nullroute
switch(config)# ip route 10.0.1.0/24 reject
switch(config)# ip route 10.0.2.0/24 20.0.0.2
switch(config)# ip route 10.0.3.0/24 1/1/1
switch(config)# ip route 10.0.3.0/24 1/1/1.110
switch(config)# ip route 10.0.2.0/24 20.0.0.2 distance 4
switch(config)# ip route 10.0.4.0/24 20.0.0.2 name AdminRoute
switch(config)# ip route 10.1.1.5/32 1/1/1 tag 20
switch(config)# ip route 1.1.2.0 255.255.255.0 2.2.2.2 track track1
switch(config)# ip route 10.1.1.6 255.255.255.0 20.1.1.2 use-forwarding-address
switch(config)# ip route 20.0.3.0/24 reject vrf test
switch(config)# ip route 10.0.4.0/24 20.0.0.2 distance 5 name AdminRoute
switch(config)# ip route 1.1.2.0 255.255.255.0 2.2.2.2 track track1 name Tracked-
Critical-Path
switch(config)# ip route 10.1.1.6 255.255.255.0 20.1.1.2 use-forwarding-address
name OSPF-Forward
switch(config)# ip route 10.0.4.0/24 20.0.0.2 tag 15 name TaggedRoute
switch(config)# ip route 20.0.4.0/24 10.0.0.2 vrf test name VRF-Management

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	The name parameter was introduced.
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ip route bfd

ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR> | <INTERFACE> | nullroute | reject]

```

    {bfd | distance | name | tag | track | use-forwarding-address | vrf}
no ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR> | <INTERFACE> | nullroute |
reject]
    {bfd | distance | name | tag | track | use-forwarding-address | vrf}

```

Description

Enables or disables BFD on the specified static route. To disable BFD, issue the command without the `bfd` option.

Parameter	Description
<DEST-IPV4-ADDR>	Specifies a route destination in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<NETMASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<NEXT-HOP-IP-ADDR>	Specifies the next hop address for reaching the destination in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<INTERFACE>	Specifies the next hop as an outgoing interface.
<code>bfd</code>	Enables BFD on the static route. Omit this parameter to disable BFD.
<code>name</code> <WORD>	Assigns a name to the destination route. Range: 1 to 64 characters.
<code>tag</code> <1-4294967295>	Specifies and assigns tag for the route.
<code>vrf</code> <DST-VRF-NAME>	The VRF route leak destination.

Examples

Enabling BFD on a static route:

```

switch(config)# interface 1/1/1
switch(config-if)# ip address 20.1.1.2/24
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# ip route 192.0.0.0/8 20.1.1.1 bfd
switch(config)# ip route 1.1.2.0 255.255.255.0 2.2.2.2 bfd name AdminRoute

```

Disabling BFD on a static route:

```

switch(config)# ip route 192.0.0.0/8 20.1.1.1

```



For more information on features that use this command, refer to the High Availability Guide or IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	The name parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ip route vrf

```
ip route <DEST-IPV4-ADDR>/<MASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
    vrf <VRF-NAME> [name <WORD>]
no ip route <DEST-IPV4-ADDR>/<MASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
    vrf <VRF-NAME> [name <WORD>]
```

Description

Adds the destination IPv4 static route on the specified VRF. If no *<VRF-NAME>* is specified the route is applied to the default VRF.

The **no** form of this command removes the IPv4 static route from the VRF.

Parameter	Description
<i><DEST-IPV4-ADDR></i>	Specifies the route destination in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<i><MASK></i>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<i><NEXT-HOP-IP-ADDR></i>	Specifies the next hop in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<i><INTERFACE></i>	Specifies the next hop as an outgoing interface.
nullroute	Silently discards packets to the destined route.
reject	Discards packets to the destined route and returns an ICMP error to the sender.
vrf <i><VRF-NAME></i>	Specifies a VRF name.
name <i><WORD></i>	Assigns a name to the destination route. Range: 1 to 64 characters.

Examples

```
switch(config)# ip route 20.0.0.0/8 10.20.30.44 vrf myvrf
switch(config)# ip route 20.1.2.0/24 1/1/30 vrf myvrf
switch(config)# ip route 1.2.3.4/32 nullroute vrf myvrf
```

```
switch(config)# ip route 1.2.3.4/32 reject vrf myvrf
switch(config)# ip route 20.0.4.0/24 10.0.0.2 vrf test name VRF-Management
```

```
switch(config)# no ip route 20.0.0.0/8 10.20.30.44 vrf myvrf
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	The name parameter was introduced.
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
9300 9300S	config	Administrators or local user group members with execution rights for this command.

ipv6 route

```
ipv6 route <DEST-IPV6-ADDR>/<NETMASK> [<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> |  
nullroute | reject]  
    {distance | name <WORD> | source <IFNAME> | tag <VALUE> | track <WORD> | vrf <WORD>}  
no ipv6 route <DEST-IPV6-ADDR>/<NETMASK> [<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> |  
nullroute | reject]  
    {distance | name <WORD> | source <IFNAME> | tag <VALUE> | track <WORD> | vrf <WORD>}
```

Description

Adds an IPv6 static route.

The **no** form of this command deletes an IPv6 static route on the default VRF.

Parameter	Description
<DEST-IPV6-ADDR>	Specifies the route destination in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<NETMASK>	Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.
<NEXTHOP-ADDR>	Specifies the next hop in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

Parameter	Description
<NEXTHOP-PORT-LAG-VLAN>	Specifies the next hop as an outgoing interface.
nullroute	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.
reject	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
distance <VALUE>	Specifies the administrative distance to associate with this static route. Range: 1 to 255. Default: 1.
name <WORD>	Specifies the name for the destination route. Range: 1 to 64 characters.
source <IFNAME>	Specifies the name for the outgoing interface.
tag <VALUE>	Specifies and assigns tag for the route. Range: 1 to 4294967295.
track <WORD>	Specifies the object monitor. Range: 1 to 64 characters.
vrf <WORD>	Specifies the VRF route leak destination.

Examples

```

switch(config)# ipv6 route 120::/124 nullroute
switch(config)# ipv6 route 122::/124 1/1/1
switch(config)# ipv6 route 122::/124 1/1/1.110
switch(config)# ipv6 route 123::/124 120::1
switch(config)# ipv6 route 122::/124 nullroute distance 5
switch(config)# ipv6 route 3001::1/128 nullroute tag 10
switch(config)# ipv6 route 122::/124 reject distance 5
switch(config)# ipv6 route 3001::1/128 reject tag 10
switch(config)# ipv6 route 123::/124 120::1 distance 6
switch(config)# ipv6 route 124::/124 120::1 name IPv6ToHost
switch(config)# ipv6 route 3002::1/128 1000::2 tag 20
switch(config)# ipv6 route 2000::/64 1000::2 track track1
switch(config)# ipv6 route 123::/124 reject vrf test
switch(config)# ipv6 route 123::/124 nullroute distance 6 name IPv6-Block
switch(config)# ipv6 route 3002::1/128 nullroute tag 11 name IPv6-Block
switch(config)# ipv6 route 123::/124 reject distance 6 name IPv6-Reject-Route
switch(config)# ipv6 route 3002::1/128 reject tag 11 name IPv6-ICMP-Error
switch(config)# ipv6 route 125::/124 120::1 distance 7 name V6ToServer
switch(config)# ipv6 route 3004::1/128 1000::3 tag 40 name Backup-Link
switch(config)# ipv6 route 2001::/64 1000::2 track track1 name IPv6-Monitored-Link
switch(config)# ipv6 route 124::/124 121::3 vrf test name IPv6-VRF-Link

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.17	The name parameter was introduced.

Release	Modification
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

show ip rib

```
show ip rib <FILTER> [vrf <VRF-NAME>]
```

Description

Shows the IPv4 Routing Information Base (RIB) of VRF with name (<VRF-NAME>). If VRF name is not specified, default VRF routes are displayed.

Parameter	Description
<FILTER>	Selects filter, see Usage section.
vrf <VRF-NAME>	Specifies the VRF name.

Usage

There are sub-options available within this command:

- **A.B.C.D:** Shows longest prefix match.
- **A.B.C.D/M:** Shows exact route match.
- **all-vrfs:** Shows all VRF information.
- **bgp:** Shows BGP routes only.
- **connected:** Shows connected routes only.
- **host-routes:** Shows ARP/ND learned routes only.
- **connected:** Shows connected routes only.
- **local:** Shows local routes only.
- **ospf:** Shows OSPF routes only.
- **rip:** Shows RIP routes only.
- **static:** Shows static routes only.
- **summary:** Shows aggregate count of routes per routing protocol.
- **vrf:** Specifies the VRF name.
- **selected:** Shows routes selected for forwarding only.
- **non-selected:** Shows routes not selected for forwarding only.

The output of the **show ip rib** commands are not available in information generated by the **show tech files** command. This information is now available in the file `ipv4_rib_dump.gz`, which can be generated using the command **sudo ovs-appctl -t hpe-routing hpe-metaswitch/show_ip_rib ipv4 all-vrfs**.

Examples

Showing IPv4 routes in RIB for HPE Aruba Networking 8325, 10000, 8360, and 9300/9300S Switch series:

```
switch# show ip rib
Origin Codes: R - RIP, O - OSPFv2, B - BGP
               C - connected, S - static, H - host-routes
Type Codes:   E - External BGP, I - Internal BGP, IA - OSPF inter area
               E1 - OSPF external type 1, E2 - OSPF external type 2
* indicates selected for forwarding

VRF: default

Prefix          Nexthop      Interface  VRF      Origin/ Distance/ Age
              Type          Metric
-----
--
*1.1.1.1/32      -             1/1/33     -         H         [1/0]
00h:00m:07s
*10.0.0.0/30      -             1/1/1      -         S         [20/0]
0d:10h:01m:41s
*10.0.1.0/30      -             1/1/1      -         B/I        [200/0]
2d:20h:01m:42s
*10.1.64.0/18     -             loopback2   -         C         [0/0]      -
*10.2.64.0/18     10.0.0.3      lag1        -         O/E1      [110/25]
1d:05h:03m:43s
*10.2.64.0/18     20.10.0.1     vlan100     -         O/E1      [110/25]
0d:05h:03m:43s
*20.1.2.3/32      2.2.2.2       1/1/4       vrf_red   B/E        [20/0]
2d:10h:01m:45s
*30.1.3.0/24      -             reject      -         S         [1/0]
33d:10h:01m:43s
*50.10.13.0/24    -             reject      -         S         [1/0]
12d:10h:01m:44s
*61.1.1.2/32      4.4.4.4       1/1/5       -         B/I        [200/0]
1d:11h:01m:45s
*62.1.1.3/32      5.5.5.5       1/1/6       -         B/I        [200/0]
0d:12h:01m:45s
*193.0.0.2/32     50.0.0.2      1/1/2       -         S         [1/0]
0d:04h:01m:43s
 193.0.0.2/32     56.0.0.3      1/1/3       -         O/E1      [110/25]
0d:04h:03m:43s

Total Route Count : 14
```

Showing IPv4 routes in RIB for all other switches:

```
switch# show ip rib
Origin Codes: R - RIP, O - OSPFv2, B - BGP
               C - connected, S - static, D - DHCP
Type Codes:   E - External BGP, I - Internal BGP, IA - OSPF inter area
               E1 - OSPF external type 1, E2 - OSPF external type 2
* indicates selected for forwarding

VRF: default

Prefix          Nexthop      Interface  VRF      Origin/ Distance/ Age
              Type          Metric
-----
--
```

```

*1.1.1.1/32      -          1/1/33      -          H      [1/0]
00h:00m:07s
*10.0.0.0/30     -          1/1/1       -          S      [20/0]
0d:10h:01m:41s
*10.0.1.0/30     -          1/1/1       -          B/I     [200/0]
2d:20h:01m:42s
*10.1.64.0/18    -          loopback2   -          C      [0/0]      -
*10.2.64.0/18    10.0.0.3    lag1      -          O/E1     [110/25]
1d:05h:03m:43s
*10.2.64.0/18    20.10.0.1   vlan100   -          O/E1     [110/25]
0d:05h:03m:43s
*20.1.2.3/32     2.2.2.2    1/1/4     vrf_red  B/E      [20/0]
2d:10h:01m:45s
*30.1.3.0/24     -          reject    -          S      [1/0]
33d:10h:01m:43s
*50.10.13.0/24   -          reject    -          S      [1/0]
12d:10h:01m:44s
*61.1.1.2/32     4.4.4.4    1/1/5     -          B/I     [200/0]
1d:11h:01m:45s
*62.1.1.3/32     5.5.5.5    1/1/6     -          B/I     [200/0]
0d:12h:01m:45s
*193.0.0.2/32    50.0.0.2   1/1/2     -          S      [1/0]
0d:04h:01m:43s
 193.0.0.2/32    56.0.0.3   1/1/3     -          O/E1     [110/25]
0d:04h:03m:43s

Total Route Count : 14

```

Showing IPv4 exact route match in RIB:

```

switch# show ip rib 10.0.0.0/30

VRF : default

Prefix      : 10.0.0.0/30          VRF(egress)      : -
Nextthop    : -                   Interface         : 1/1/1
Origin       : Connected           Type              : -
Distance     : 0                   Metric            : 0
Age          : -                   Tag               : 0
Selected     : Yes                 Recursive Nexthop  : No

```

Showing IPv4 RIB summary:

```

switch# show ip rib summary

IPv4 RIB Table Summary

VRF name :      default
Protocol  RIB Routes
-----
connected 1010
local     1011
host-routes 2
static    4
ospfv2    509
bgp       9014
selected  10008
non-selected 1518

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.12	Added host-routes parameter and updated output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip rib host-routes

show ip rib host-routes[vrf <VRF-NAME>]

Description

Shows the IPv4 host-routes Routing Information Base (RIB) routes of VRF with name (<VRF-NAME>). If VRF name is not specified, default VRF routes are displayed.

Parameter	Description
<VRF>	Displays the routes in the VRF.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Showing IPv4 routes in RIB:

```
switch# show ipv4 rib host-routes
Displaying ipv4 routes in RIB
Origin Codes: R - RIP, O - OSPFv2, B - BGP
               C - connected, S - static, L - local, H - host-routes
Type Codes:   E - External BGP, I - Internal BGP
               IA - OSPF inter area, ia - OSPF intra area
               E1 - OSPF external type 1, E2 - OSPF external type 2
* indicates selected for forwarding
VRF: default
Prefix      Nexthop      Interface      VRF(egress)      Origin/
Distance/   Age                                     Type
Metric
-----
*1.1.1.2/32      1.1.1.2          1/1/1          -                  H          [1/0]
```

00h:08m:35s
Total Route Count : 1

Command History

Release	Modification
10.12	Command introduced.

Command Information

Platforms	Command context	Authority
9300	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ipv6 rib

```
show ipv6 rib <FILTER> [vrf <VRF-NAME>]
```

Description

Shows the IPv6 Routing Information Base (RIB) of VRF with name (<VRF-NAME>). If VRF name is not specified, default VRF routes are displayed.

Parameter	Description
<FILTER>	Selects filter, see usage section.
vrf <VRF-NAME>	Shows routes in the VRF and specifies VRF name.

Usage

There are sub-options available within this command:

- **X:X:X:X:** Shows longest prefix match.
- **X:X:X:X/M:** Shows exact route match.
- **all-vrfs:** Shows all VRF information.
- **bgp:** Shows BGP routes only.
- **connected:** Shows connected routes only.
- **host-routes:** Show ARP/ND learned routes only.
- **local:** Shows local routes only.
- **ospf:** Shows OSPF routes only.
- **rip:** Shows RIP routes only.
- **static:** Shows static routes only.
- **summary:** Shows aggregate count of routes per routing protocol.
- **vrf:** Specifies the VRF name.
- **selected:** Shows routes selected for forwarding only.
- **non-selected:** Shows routes not selected for forwarding only.

Examples

Showing IPv6 routes in RIB for HPE Aruba Networking 8325, 10000, 8360, and 9300/9300S Switch series:

```
switch# show ipv6 rib
Origin Codes: R - RIPng, O - OSPFv3, B - BGP
               C - connected, S - static, H - host-routes
Type Codes:   E - External BGP, I - Internal BGP, IA - OSPF inter area
               E1 - OSPF external type 1, E2 - OSPF external type 2
* indicates selected for forwarding

VRF: default

Prefix          Nexthop    Interface  VRF      Origin/ Distance/ Age
              Type      Metric
-----
--
*1::2/128       1::2      1/1/1      -        H        [1/0]      00h:00m:06s
*1000::/64      -         1/1/1      -        C        [0/0]      -
*1000::8/128    -         1/1/1      -        L        [0/0]      -
*1001::db8::/32 1000::10  1/1/1      -        B/I      [200/0]    1d:20h:01m:42s
*2000::/64      fe80::3182 vlan100     -        S        [1/0]      2d:05h:03m:43s
 2000::/64      fe80::1241 1/1/1      -        O/E1     [110/25]   0d:05h:03m:43s
*2000::2000:0:0:0/67 fe80::1111 lag1       Green     B/E      [20/0]    1d:10h:01m:45s
*3001::0/64     -         vlan100     -        C        [0/0]      -
*3001::1/128    -         vlan100     -        L        [0/0]      -
*6101::0/64     -         nullroute   -        S        [1/0]      -
12d:10h:01m:43s

Total Route Count : 10
```

Showing IPv6 routes in RIB for the other switch series:

```
switch# show ipv6 rib
Origin Codes: R - RIPng, O - OSPFv3, B - BGP
               C - connected, S - static, D- DHCP
Type Codes:   E - External BGP, I - Internal BGP, IA - OSPF inter area
               E1 - OSPF external type 1, E2 - OSPF external type 2
* indicates selected for forwarding

VRF: default

Prefix          Nexthop    Interface  VRF      Origin/ Distance/ Age
              Type      Metric
-----
--
*1000::/64      -         1/1/1      -        C        [0/0]      -
*1000::8/128    -         1/1/1      -        L        [0/0]      -
*1001::db8::/32 1000::10  1/1/1      -        B/I      [200/0]    1d:20h:01m:42s
*2000::/64      fe80::3182 vlan100     -        S        [1/0]      2d:05h:03m:43s
 2000::/64      fe80::1241 1/1/1      -        O/E1     [110/25]   0d:05h:03m:43s
*2000::2000:0:0:0/67 fe80::1111 lag1       Green     B/E      [20/0]    1d:10h:01m:45s
*3001::0/64     -         vlan100     -        C        [0/0]      -
*3001::1/128    -         vlan100     -        L        [0/0]      -
*6101::0/64     -         nullroute   -        S        [1/0]      -
12d:10h:01m:43s

Total Route Count : 10
```

Showing IPv6 exact route match in RIB:

```
switch# show ipv6 rib 2000::2000:0:0:0

VRF : default

Prefix          : 2000::2000:0:0:0/67      VRF (egress)    : Green
Nexthop         : fe80::1111               Interface       : lag1
Origin          : BGP                      Type            : External
Distance        : 20                      Metric          : 0
Age             : 1d:10h:01m:45s           Tag            : 20
Selected        : Yes                     Recursive Nexthop : Yes
```

Showing IPv6 RIB summary:

```
switch# show ipv6 rib summary

IPv6 RIB Table Summary

VRF name : default
  Protocol    RIB Routes
-----
connected    1009
local        1010
static        3
host-routes   1
ospfv3       508
bgp          1013

selected     10004
non-selected 1527
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.12	Added host-routes parameter and updated output.
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ipv6 rib host-routes

```
show ipv6 rib host-routes[vrf <VRF-NAME>]
```

Description

Shows the IPv6 host-routes Routing Information Base (RIB) routes of VRF with name (<VRF-NAME>). If VRF name is not specified, default VRF routes are displayed.

Parameter	Description
<VRF>	Displays the routes in the VRF.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Showing IPv6 routes in RIB:

```
switch# show ipv6 rib host-routes
Displaying ipv6 routes in RIB
Origin Codes: R - RIP, O - OSPFv2, B - BGP
               C - connected, S - static, L - local, H - host-routes
Type Codes:   E - External BGP, I - Internal BGP
               IA - OSPF inter area, ia - OSPF intra area
               E1 - OSPF external type 1, E2 - OSPF external type 2
* indicates selected for forwarding
VRF: default
Prefix          Nexthop          Interface      VRF (egress)      Origin/
Distance/      Age                                     Type
Metric
-----
*1::2/128      1::2                          1/1/1         -                  H
[1/0]          00h:48m:08s
Total Route Count : 1
```
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.12   | Command introduced. |

## Command Information

| Platforms | Command context             | Authority                                                                          |
|-----------|-----------------------------|------------------------------------------------------------------------------------|
| 9300      | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

## ipv6 route vrf

```
ipv6 route <DEST-IPV6-ADDR>/<PREFIX> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
vrf <VRF-NAME> [name <WORD>]
no ipv6 route <DEST-IPV6-ADDR>/<PREFIX> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
vrf <VRF-NAME> [name <WORD>]
```

## Description

Adds an IPv6 static route in the specified VRF. If no *<VRF-NAME>* is specified it is added to the default VRF.

The **no** form of this command removes an IPv6 static route from the VRF.

| Parameter                         | Description                                                                                                                                    |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;DEST-IPV6-ADDR&gt;</i>     | Specifies an IP address in IPv6 format ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> is a hexadecimal number from 0 to F. |
| <i>&lt;MASK&gt;</i>               | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 128.                |
| <i>&lt;NEXT-HOP-IP-ADDR&gt;</i>   | Specifies the next hop in IPv6 format ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> is a hexadecimal number from 0 to F.  |
| <i>&lt;INTERFACE&gt;</i>          | Specifies the next hop as an outgoing interface.                                                                                               |
| <code>nullroute</code>            | Specifies that packets matching the destination prefix are silently discarded and no ICMP error notification is sent to the sender.            |
| <code>reject</code>               | Specifies that packets matching the destination prefix are discarded and an ICMP error notification is sent to the sender.                     |
| <code>vrf &lt;VRF-NAME&gt;</code> | Specifies the name of a VRF. Default: default.                                                                                                 |
| <code>name &lt;WORD&gt;</code>    | Assigns a name to the destination route. Range: 1 to 64 characters.                                                                            |

## Examples

```
switch(config)# ipv6 route 120::/124 121::2 vrf test
switch(config)# ipv6 route 121::/124 1/1/9 vrf test
switch(config)# ipv6 route 122::/124 nullroute vrf test
switch(config)# ipv6 route 123::/124 reject vrf test
switch(config)# ipv6 route 124::/124 121::3 vrf test name IPv6-VRF-Link
```

```
switch(config)# no ipv6 route 120::/124 121::2 vrf test
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                              |
|------------------|-------------------------------------------|
| 10.17            | The <b>name</b> parameter was introduced. |
| 10.10            | Inclusive language update.                |
| 10.07 or earlier | --                                        |

## Command Information



| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## show ip route

show ip route [<**A.B.C.D**> | <**A.B.C.D/M**> | all-vrfs | bgp | connected | local | ospf | static | summary | vrf <*VRF-NAME*> [vsx-peer] | protected]

### Description

Displays IP route tables.

| Parameter               | Description                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------|
| < <b>A.B.C.D</b> >      | Display longest prefix match.                                                                   |
| < <b>A.B.C.D/M</b> >    | Display exact route match.                                                                      |
| all-vrfs                | Display information for all VRFs.                                                               |
| bgp                     | Display bgp routes only.                                                                        |
| connected               | Display connected routes only.                                                                  |
| local                   | Display local routes only.                                                                      |
| ospf                    | Display ospf routes only.                                                                       |
| protected               | Display protected routes only.                                                                  |
| static                  | Display static routes only.                                                                     |
| summary                 | Display the aggregate count of routes per routing protocol.                                     |
| vrf < <i>vrf-name</i> > | Specify a VRF by VRF name (if no < <i>VRF-NAME</i> > is specified, the default VRF is implied). |

### Examples

Showing IP routes:

```
dut1# show ip route all-vrfs

Displaying ip routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
 R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
 IA - OSPF internal area, E1 - OSPF external type 1
 E2 - OSPF external type 2
FRR: + - Backup Nexthop
 * - data obtainable via 'show bgp ip unicast A.B.C.D/M'

VRF: 1
```

| Prefix                 | Nexthop  | Interface | VRF (egress) | Origin/<br>Type | Distance/<br>Metric | Age         |
|------------------------|----------|-----------|--------------|-----------------|---------------------|-------------|
| -----                  |          |           |              |                 |                     |             |
| --                     |          |           |              |                 |                     |             |
| 1.1.1.0/24             | -        | 1/1/22    | -            | C               | [0/0]               | -           |
| 1.1.1.1/32             | -        | 1/1/22    | -            | L               | [0/0]               | -           |
| 1.1.2.0/24             | -        | 1/1/23    | -            | C               | [0/0]               | -           |
| 1.1.2.1/32             | -        | 1/1/23    | -            | L               | [0/0]               | -           |
| 1.1.5.0/24             | -        | 1/1/25    | -            | C               | [0/0]               | -           |
| 1.1.5.1/32             | -        | 1/1/25    | -            | L               | [0/0]               | -           |
| 200.1.0.0/24           | 1.1.2.2  | 1/1/23    | -            | B/E             | [20/0]              | 00h:00m:13s |
|                        | 1.1.1.2+ | 1/1/22    | -            | B/*             | [*/0]               | 00h:00m:13s |
| 200.1.1.0/24           | 1.1.2.2  | 1/1/23    | -            | B/E             | [20/0]              | 00h:00m:13s |
|                        | 1.1.1.2+ | 1/1/22    | -            | B/*             | [*/0]               | 00h:00m:13s |
| 200.1.2.0/24           | 1.1.2.2  | 1/1/23    | -            | B/E             | [20/0]              | 00h:00m:13s |
|                        | 1.1.1.2+ | 1/1/22    | -            | B/*             | [*/0]               | 00h:00m:13s |
| 200.1.3.0/24           | 1.1.2.2  | 1/1/23    | -            | B/E             | [20/0]              | 00h:00m:13s |
|                        | 1.1.1.2+ | 1/1/22    | -            | B/*             | [*/0]               | 00h:00m:13s |
| 200.1.4.0/24           | 1.1.2.2  | 1/1/23    | -            | B/E             | [20/0]              | 00h:00m:13s |
|                        | 1.1.1.2+ | 1/1/22    | -            | B/*             | [*/0]               | 00h:00m:13s |
| Total Route Count : 11 |          |           |              |                 |                     |             |

Showing ip protected routes:

```
switch# show ip route protected
all-vrfs all vrf information
vrf Specify the VRF name
<cr>
```

Showing protected routes for all vrfs:




---

Protected routes are only supported on the 9300 Switch Series.

---

```
switch# show ip route protected all-vrfs

Displaying ip routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
 R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
 IA - OSPF internal area, E1 - OSPF external type 1
 E2 - OSPF external type 2
FRR: + - Backup Nexthop
 * - data obtainable via 'show bgp ip unicast A.B.C.D/M'

VRF: default
```

| Prefix           | Nexthop        | Interface | VRF(egress) | Origin/<br>Type | Distance/<br>Metric | Age         |
|------------------|----------------|-----------|-------------|-----------------|---------------------|-------------|
| -----            |                |           |             |                 |                     |             |
| --               |                |           |             |                 |                     |             |
| 120.120.120.0/24 | 110.110.110.1  | vlan20    | -           | O               | [110/120]           |             |
| 03h:35m:55s      |                |           |             |                 |                     |             |
|                  | 130.130.130.1+ | vlan22    | -           | B/*             | [*/120]             | 03h:35m:55s |

```

140.140.140.0/24 130.130.130.1 vlan22 - O [110/130]
03h:25m:13s
110.110.110.1+ vlan20 - B/* [*/130] 03h:25m:13s
211.0.0.0/24 110.110.110.1 vlan20 - O [110/122]
03h:25m:13s
130.130.130.1+ vlan22 - B/* [*/122] 03h:25m:13s

VRF: red

150.150.150.0/24 120.120.120.1 vlan21 - O [110/120]
03h:35m:55s
140.140.140.1+ vlan23 - B/* [*/120] 03h:35m:55s

Total Route Count : 4

```

Showing protected routes for a specific vrf, **vrf red**:

```

switch# show ip route protected vrf red

Displaying ip routes selected for forwarding
Origin Codes: C - connected, S - static, L - local
 R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
 IA - OSPF internal area, E1 - OSPF external type 1
 E2 - OSPF external type 2
FRR: + - Backup Nexthop
 * - data obtainable via 'show bgp ip unicast A.B.C.D/M'

VRF: red

Prefix Nexthop Interface VRF(egress) Origin/ Distance/ Age
 Nexthop Interface VRF(egress) Type Metric

--
150.150.150.0/24 121.120.120.1 vlan21 - O [110/120
03h:35m:55s
 141.140.140.1+ vlan23 - B/* [*/120] 03h:35m:55s

Total Route Count : 1

```

Show IP routes for a specific IP address:

```

dut1# show ip route 200.1.0.0/24 vrf 1

VRF: 1

Prefix : 200.1.0.0/24 VRF(egress)
: -
Nexthop : 1.1.2.2 Interface
: 1/1/6
Origin : bgp Type
: bgp_ext
Distance : 20 Metric
: 0
Age : 00h:00m:22s Tag
: 0
Encap Type : - Encap Details
: -
Nexthop Type : Primary

```

```

Prefix : 200.1.0.0/24 VRF (egress)
: -
Nexthop : 1.1.1.2 Interface
: 1/1/2
Origin : bgp Type
: *
Distance : * Metric
: 0
Age : 00h:00m:22s Tag
: 0
Encap Type : - Encap Details
: -
Nexthop Type : Backup

* - data for backup nexthop obtainable via 'show bgp ip unicast A.B.C.D/M'

```

Showing the ip route summary for all vrfs:

```

core1# show ip route summary all-vrfs

IP Route Table Summary

VRF name : red
Protocol Active Routes Protected Routes

connected 3 -
local 3 -
bgp 12 5

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                                     |
|------------------|--------------------------------------------------|
| 10.14.1000       | Added protected paramater to 9300 Switch Series. |
| 10.07 or earlier | --                                               |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ipv6 route

```

show ipv6 route [<X.X.X.X> | <X.X.X.X/M> | all-vrfs | bgp | connected | local | ospf |
static | summary | vrf <vrf-name>] [vsx-peer]

```

## Description

Displays IPv6 route tables.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <X.X.X.X>      | Display exact route match.                                                                                                                                                                                                       |
| <X.X.X.X/M>    | Display exact route match.                                                                                                                                                                                                       |
| all-vrfs       | Display information for all VRFs.                                                                                                                                                                                                |
| bgp            | Display bgp routes only.                                                                                                                                                                                                         |
| connected      | Display connected routes only.                                                                                                                                                                                                   |
| local          | Display local routes only.                                                                                                                                                                                                       |
| ospf           | Display ospf routes only.                                                                                                                                                                                                        |
| static         | Display static routes only.                                                                                                                                                                                                      |
| summary        | Display the aggregate count of routes per routing protocol.                                                                                                                                                                      |
| vrf <vrf-name> | Specify a VRF by VRF name (if no <VRF-NAME> is specified, the default VRF is implied).                                                                                                                                           |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

Showing IPv6 route tables:

```
switch# show ipv6 route

Displaying ipv6 routes selected for forwarding

'[x/y]' denotes [distance/metric]

1000::/64, vrf default
 via vlan2, [0/0], connected
1000::1/128, vrf default
 via vlan2, [0/0], local
2000::/64, vrf default
 via vlan2, [1/0], static
2001::/64, vrf default
 via 1000::2, [1/0], static
3000:2301::/64, vrf default
 nullroute, [1/0], static
4000:2301::/64, vrf default
 reject route, [1/0], static
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification               |
|------------------|----------------------------|
| 10.10            | Inclusive language update. |
| 10.07 or earlier | --                         |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## encapsulation dot1q

```
encapsulation dot1q <VLAN-ID>
no encapsulation dot1q <VLAN-ID>
```

### Description

Configures 802.1Q encapsulation on a subinterface.  
The **no** form of this command removes 802.1Q encapsulation on a subinterface.

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <VLAN-ID> | Specifies encapsulation VLAN ID.<br>Range 1 to 4094.<br><br><b>NOTE:</b> The encapsulation VLAN ID should be unique within an L3 LAG subinterface. The same encapsulation VLAN ID can be configured among different parent interfaces, but the encapsulation VLAN ID should not be configured in the internal VLAN range. (Encapsulation VLAN IDs and static VLANs are entirely different and do not coincide.) |

### Usage

Associates an 802.1Q VLAN ID with a subinterface.

### Examples

Configuring 802.1Q encapsulation on a subinterface:

```
switch(config)# interface 1/1/1.201
switch(config-subif)# encapsulation dot1q 10
```

Removing 802.1Q encapsulation on a subinterface:

```
switch(config-subif)# no encapsulation dot1q 10
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification                               |
|---------|--------------------------------------------|
| 10.16   | Command introduced for 9300 Switch series. |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config-subif    | Administrators or local user group members with execution rights for this command. |

## interface

```
interface <IFNAME>.<ID>
no interface <IFNAME>.<ID>
```

```
interface lag <LAGNUM>.<ID>
no interface lag <LAGNUM>.<ID>
```

## Description

Creates a subinterface on an L3 interface and enters subinterface configuration mode. The subinterface name consists of the parent interface name (for example, 1/1/1) followed by a period and a unique ID number.

The **no** form of these commands deletes a subinterface from an L3 interface.

8325, 8325H, 8325P, and 10000 Switch series require an internal VLAN for every subinterface, in addition to the internal VLANs used for other purposes. For example, to support 1024 subinterfaces, an internal VLAN range that is at least that large must be reserved using the **system internal-vlan-range** command. 8325, 8325H, 8325P, and 10000 Series switches support a maximum of 1024 subinterfaces resources.

BFD sessions are not supported on sub interfaces on 9300 Switch series. Use switch virtual interfaces (SVIs) to configure a BFD session on these switch models.

| Parameter | Description                                 |
|-----------|---------------------------------------------|
| <IFNAME>  | Specifies L3 interface name.                |
| <ID>      | Specifies subinterface ID. Range 1 to 4094. |
| <LAGNUM>  | Specifies L3 LAG interface number.          |

## Usage

To create a LAG subinterface, the parent LAG must exist before creating the subinterface.

## Examples

Creating a subinterface on L3 interface 1/1/1.201 and entering subinterface configuration mode:

```
switch(config)# interface 1/1/1.201
switch(config-subif)#
```



Deleting subinterface on L3 interface 1/1/1.201:

```
switch(config)# no interface 1/1/1.201
```

Creating a subinterface on an L3 LAG port and entering subinterface configuration mode:

```
switch(config)# interface lag 1
switch(config-if)# interface lag 1.201
switch(config-subif)#
```

Deleting subinterface on an L3 LAG port :

```
switch(config)# no interface lag 1.201
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                               |
|---------|--------------------------------------------|
| 10.16   | Command introduced for 9300 Switch series. |

## Command Information

| Platforms | Command context | Authority                                                                          |
|-----------|-----------------|------------------------------------------------------------------------------------|
| 9300      | config          | Administrators or local user group members with execution rights for this command. |

## show capacities subinterface

show capacities subinterface

### Description

Displays maximum subinterface capacity.

### Examples

Showing maximum subinterface capacity:

```
switch# show capacities subinterface

System Capacities: Filter Subinterface
Capacities Name
Value

-
```

```
Maximum number of LAG subinterfaces for the entire system
256
Maximum number of LAG members when the LAG has subinterfaces
4
Maximum number of normal subinterfaces for the entire system
1024
Maximum number of subinterface resources for the entire system (normal+(4*LAG)
1024
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                               |
|---------|--------------------------------------------|
| 10.16   | Command introduced for 9300 Switch series. |

## Command Information

| Platforms | Command context             | Authority                                                                                                                                                                  |
|-----------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300      | Operator (>) or Manager (#) | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

## show interface

```
show interface <IFNAME>.<ID>
show interface lag <LAGNUM>.<ID>
```

## Description

Displays a subinterface configuration.

| Parameter | Description                        |
|-----------|------------------------------------|
| <IFNAME>  | Specifies L3 interface name.       |
| <ID>      | Specifies subinterface ID.         |
| <LAGNUM>  | Specifies L3 LAG interface number. |

## Examples

Showing subinterface configuration:

```
switch# show interface 1/1/1.201
Interface 1/1/1.201 is down
Admin state is up
State information: Waiting for link
Description:
```

```

Hardware: Ethernet, MAC Address: 38:21:c7:5a:80:80
Encapsulation dot1Q ID: 10
Statistic RX TX Total

L3 Packets 0 0 0
L3 Bytes 0 0 0

```

Showing subinterface LAG configuration:

```

switch# show interface lag1.1
Interface lag1.1 is down
Admin state is up
Description:
Hardware: Ethernet, MAC Address: 38:21:c7:5a:80:80
Encapsulation dot1Q ID: 2
Statistic RX TX Total

L3 Packets 0 0 0
L3 Bytes 0 0 0

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                               |
|---------|--------------------------------------------|
| 10.16   | Command introduced for 9300 Switch series. |

## Command Information

| Platforms | Command context             | Authority                                                                                                                                                                  |
|-----------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300      | Operator (>) or Manager (#) | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

### copy checkpoint

copy checkpoint <CHECKPOINT-NAME> {<STORAGE-URL> | <REMOTE-URL>}

#### Description

Copies the checkpoint using TFTP, SFTP, SCP, or USB.

| Parameter                      | Description                                                                                                                                                                                                                                                                                                        |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <CHECKPOINT-NAME>              | Specifies the checkpoint name.                                                                                                                                                                                                                                                                                     |
| {<STORAGE-URL>   <REMOTE-URL>} | Select either the storage URL or the remote URL for the destination of the copied command output. Required.                                                                                                                                                                                                        |
| <STORAGE-URL>                  | Specifies the USB to copy command output.<br>Syntax:<br><b>{usb}:/&lt;FILE&gt;</b>                                                                                                                                                                                                                                 |
| <REMOTE-URL>                   | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"><li>▪ <b>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;][;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</b></li><li>▪ <b>{sftp://   scp://&lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</b></li></ul> |

#### Examples

Copying checkpoint chpt to a remote URL:

```
switch# copy checkpoint chpt scp://root@10.0.1.1/config vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

#### Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

#### Command Information

| Platforms     | Command context | Authority                                                                                                                                                                  |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

## copy command-output

copy command-output "<COMMAND>" {<STORAGE-URL> | <REMOTE-URL> [vrf <VRF-NAME>]}

### Description

Copies the specified command output using TFTP, SFTP, SCP, USB, or local.

| Parameter                                       | Description                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <COMMAND>                                       | Specifies the command from which you want to obtain its output. Required. Users with auditor rights can specify these two commands only:<br><b>show accounting log</b><br><b>show events</b>                                                                                                                         |
| {<STORAGE-URL>   <REMOTE-URL> [vrf <VRF-NAME>]} | Select either the storage URL or the remote URL for the destination of the copied command output. Required.                                                                                                                                                                                                          |
| <STORAGE-URL>                                   | Specifies the USB to copy command output.<br>Syntax:<br><b>{usb}:/&lt;FILE&gt;</b>                                                                                                                                                                                                                                   |
| <REMOTE-URL>                                    | Specifies the URL to copy the command output.<br>Syntax:<br><ul style="list-style-type: none"> <li><b>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;][;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</b></li> <li><b>{sftp://   scp://&lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</b></li> </ul> |
| vrf <VRF-NAME>                                  | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                   |

### Examples

Copying the output from the **show events** command to a remote URL:

```
switch# copy command-output "show events" tftp://10.100.0.12/file
```

Copying the output from the **show tech** command to a remote URL with a VRF named *mgmt*:

```
switch# copy command-output "show tech" scp://user@10.100.0.12/file vrf mgmt
```

Copying the output from the **show tech** command to a remote URL with a VRF named *mgmt*:

```
switch# copy command-output "show tech" tftp://10.100.0.12/file vrf mgmt
```

Copying the output from the **show events** command to a file named **events** on a USB drive:

```
switch# copy command-output "show events" usb:/events
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                                  |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

# copy core-dump daemon

```
copy core-dump daemon <DAEMON-NAME>[:<INSTANCE-ID>] <REMOTE-URL> [vrf <VRF-NAME>]
```

## Description

Copies the core-dump from the specified daemon using TFTP, SFTP, SCP, USB, or local.

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DAEMON-NAME>     | Specifies the name of the daemon. Required.                                                                                                                                                                                                                                                                                                 |
| [ :<INSTANCE-ID>] | Specifies the instance of the daemon core dump. Optional.                                                                                                                                                                                                                                                                                   |
| <REMOTE_URL>      | Specifies the remote destination URL. Required. The syntax of the URL is the following:<br>Syntax: <ul style="list-style-type: none"><li>▪ {tftp://}&lt;IP&gt;   &lt;HOST&gt;]:&lt;PORT&gt;][:blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</li><li>▪ {sftp://   scp:// &lt;USER&gt;@}&lt;IP&gt;   &lt;HOST&gt;]:&lt;PORT&gt;]/&lt;FILE&gt;</li></ul> |
| vrf <VRF-NAME>    | Specifies the VRF name. If no VRF name is provided, the VRF named <i>default</i> is used. Optional.                                                                                                                                                                                                                                         |

## Examples

Copying the core dump from daemon ops-vland to a remote URL with a VRF named mgmt:

```
switch# copy core-dump daemon ops-vland sftp://abc@10.0.14.211/vland_coredump.xz
vrf mgmt
```

Copying the core dump from daemon ops-vland to a remote URL with a VRF named mgmt:

```
switch# copy core-dump daemon ops-vland scp://abc@10.0.14.211/vland_coredump.xz
vrf mgmt
```

Copying the core dump from daemon ops-switchd to a USB drive:

```
switch# copy core-dump daemon ops-switchd usb:/switchd\
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy core-dump kernel

copy core-dump kernel <REMOTE-URL> [vrf <VRF-NAME>]

## Description

Copies a kernel core dump using TFTP, SFTP, or local.

| Parameter      | Description                                                                                                                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <REMOTE-URL>   | Specifies the URL to copy the command output. Required.<br>Syntax: <ul style="list-style-type: none"><li>▪ {tftp://}{&lt;IP&gt;   &lt;HOST&gt;}:{&lt;PORT&gt;}[:&lt;blocksize=&lt;VAL&gt;]/{&lt;FILE&gt;}</li><li>▪ {sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}:{&lt;PORT&gt;}/{&lt;FILE&gt;}</li></ul> |
| vrf <VRF-NAME> | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                      |

## Examples

Copying the kernel core dump to the URL:

```
switch# copy core-dump kernel tftp://10.100.0.12/kernel_dump.tar.gz
```

Copying the kernel core dump to the URL with the VRF named mgmt:

```
switch# copy core-dump kernel tftp://10.100.0.12/kernel_dump.tar.gz vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy core-dump kernel <STORAGE-URL>

copy core-dump kernel <STORAGE-URL>

### Description

Copies the kernel core dump to a USB drive or local.

| Parameter     | Description                                                                               |
|---------------|-------------------------------------------------------------------------------------------|
| <STORAGE-URL> | Specifies the USB to copy command output. Required.<br>Syntax: <b>{usb}:/&lt;FILE&gt;</b> |

### Examples

Copying the kernel core dump to a USB drive:

```
switch# copy core-dump kernel usb:/kernel.tar.gz
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |



## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy diag-dump feature <FEATURE>

copy diag-dump feature <FEATURE> {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}

### Description

Copies the specified diagnostic information using TFTP, SFTP, SCP, USB, or local.

| Parameter                                       | Description                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <FEATURE>                                       | The name of a feature, for example <b>aaa</b> or <b>vrmp</b> . Required.                                                                                                                                                                                                                                                                           |
| {<REMOTE-URL> [vrf <VRF-NAME>]   <STORAGE-URL>} | Select either the remote URL or the storage URL for the destination of the copied command output. Required.                                                                                                                                                                                                                                        |
| <REMOTE-URL>                                    | Specifies the remote destination URL. Required. The syntax of the URL is the following:<br>Syntax:<br><ul style="list-style-type: none"><li>▪ {tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;][;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</li><li>▪ {sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</li></ul> |
| vrf <VRF-NAME>                                  | Specifies the VRF name. If no VRF name is provided, the VRF named <i>default</i> is used. Optional.                                                                                                                                                                                                                                                |
| <STORAGE-URL>                                   | Specifies the USB to copy command output. Required.<br>Syntax: {usb} : /<FILE>                                                                                                                                                                                                                                                                     |

### Examples

Copying the output from the aaa feature to a remote URL with a specified VRF:

```
switch# copy diag-dump feature aaa tftp://10.100.0.12/diagdump.txt vrf mgmt
```

Copying the output from the aaa feature to a remote URL with a specified VRF:

```
switch# copy diag-dump feature aaa scp://user@10.100.0.12/diagdump.txt vrf mgmt
```

Copying the output from the vrrp feature to a USB drive:

```
switch# copy diag-dump feature vrrp usb:/diagdump.txt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy diag-dump local-file

```
copy diag-dump local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

### Description

Copies the diagnostic information stored in a local file using TFTP, SFTP, SCP, USB, or local.

| Parameter                                       | Description                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {<REMOTE-URL> [vrf <VRF-NAME>]   <STORAGE-URL>} | Select either the storage URL or the remote URL for the destination of the copied command output. Required.                                                                                                                                                                                           |
| <REMOTE-URL>                                    | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"><li>▪ {tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;][;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</li><li>▪ {sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</li></ul> |
| vrf <VRF-NAME>                                  | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                    |
| <STORAGE-URL>                                   | Specifies the USB to copy command output.<br>Syntax: {usb:}/<FILE>                                                                                                                                                                                                                                    |

### Usage

The **copy diag-dump local-file** command can be used only after the information is captured. Run the **diag-dump <FEATURE-NAME> basic local-file** command before you enter the **copy diag-dump local-file** command to capture the diagnostic information for the specified feature into the local file.

## Examples

Copying the output from the local file to a remote URL:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file tftp://10.100.0.12/diagdump.txt
```

Copying the output from the local file to a remote URL:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file scp://user@10.100.0.12/diagdump.txt
```

Copying the output from the local file to a USB drive:

```
switch# diag-dump aaa basic local-file
switch# copy diag-dump local-file usb:/diagdump.txt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy <IMAGE>

copy <IMAGE> {<STORAGE-URL> | <REMOTE-URL>} <FILE-NAME> [vrf <VRF-NAME>]

## Description

Copies the image using TFTP, SFTP, SCP, or USB.

| Parameter                        | Description                                                                                                                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IMAGE>                          | Specifies the image.                                                                                                                                                                                                                                                                                                       |
| { <STORAGE-URL>   <REMOTE-URL> } | Select either the storage URL or the remote URL for the destination of the copied command output. Required.                                                                                                                                                                                                                |
| <STORAGE-URL>                    | Specifies the USB to copy command output.<br>Syntax:<br><b>{usb}:/&lt;FILE&gt;</b>                                                                                                                                                                                                                                         |
| <REMOTE-URL>                     | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"> <li>▪ <b>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}{[:&lt;PORT&gt;][:blocksize=&lt;VAL&gt;]}/&lt;FILE&gt;</b></li> <li>▪ <b>{sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}{[:&lt;PORT&gt;]}/&lt;FILE&gt;</b></li> </ul> |
| <FILE-NAME>                      | Specifies the file name.                                                                                                                                                                                                                                                                                                   |
| vrf <VRF-NAME>                   | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                         |

## Examples

Copying the image to a remote URL:

```
switch# copy scp://root@20.0.1.1/primary.swi primary vrf mgmt
```

Copying the secondary image to a remote URL:

```
switch# copy secondary scp://root@20.0.1.1/primary.swi vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                                  |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

## copy running-config

```
copy running-config {<STORAGE-URL> | <REMOTE-URL>}/config <CONFIG-NAME> [vrf <VRF-NAME>]
```

## Description

Copies the running configuration using TFTP, SFTP, SCP, or USB.

| Parameter                      | Description                                                                                                                                                                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {<STORAGE-URL>   <REMOTE-URL>} | Select either the storage URL or the remote URL for the destination of the copied command output. Required.                                                                                                                                                                                          |
| <STORAGE-URL>                  | Specifies the USB to copy command output.<br>Syntax:<br><b>{usb}:/&lt;FILE&gt;</b>                                                                                                                                                                                                                   |
| <REMOTE-URL>                   | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"><li>▪ {tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;][;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</li><li>▪ {sftp://   scp://&lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</li></ul> |
| config <CONFIG-NAME>           | Specifies the running configuration.                                                                                                                                                                                                                                                                 |
| vrf <VRF-NAME>                 | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                   |
| overwrite                      | The configuration is only applied to the running configuration if all commands succeed without errors.                                                                                                                                                                                               |

## Usage

By default, the CLI configuration contained in the remote file is applied on top of the running configuration, and all the CLI commands in the file are applied line-by-line. If a particular CLI command fails, the failure is logged in the event log and the next line in the CLI configuration is processed.

When using the optional **overwrite** parameter, the configuration is only applied to running configuration if *all* the commands succeeded without errors. If errors are present, the existing running-config will remain intact. You can then inspect the event logs to check and fix the errors and retry the operation. If more than 20 errors are present, the operation stops processing any further commands, and will display the errors at that point in the event logs. For more information on this feature, refer to the video on the [HPE Aruba Networking Airheads Broadcasting Channel](#).

## Examples

Copying the running configuration to a remote URL:

```
switch# copy running-config scp://root@10.0.1.1/config cli vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release | Modification                           |
|---------|----------------------------------------|
| 10.15   | The overwrite parameter is introduced. |

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                                  |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

## copy show-tech feature

`copy show-tech feature <FEATURE> {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}`

### Description

Copies show tech output using TFTP, SFTP, SCP, USB, or local.

| Parameter                                                                      | Description                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>{&lt;REMOTE-URL&gt; [vrf &lt;VRF-NAME&gt;   &lt;STORAGE-URL&gt;]}</code> | Select either the remote URL or the storage URL for the destination of the copied command output. Required.                                                                                                                                                                                                                                      |
| <code>&lt;REMOTE-URL&gt;</code>                                                | Specifies the URL to copy the command output. Required.<br>Syntax:<br><ul style="list-style-type: none"> <li><code>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}{[:&lt;PORT&gt;] [;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;}</code></li> <li><code>{sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}{[:&lt;PORT&gt;]/&lt;FILE&gt;}</code></li> </ul> |
| <code>vrf &lt;VRF-NAME&gt;</code>                                              | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                                               |
| <code>&lt;STORAGE-URL&gt;</code>                                               | Specifies the USB to copy command output. Required.<br>Syntax: <code>{usb}/&lt;FILE&gt;</code>                                                                                                                                                                                                                                                   |

### Example

Copying show tech output of the **aaa** feature using SCP:

```
switch# copy show-tech feature aaa scp://user@10.0.0.12/file.txt vrf mgmt
```

Copying show tech output of the `config` feature using SFTP on the `mgmt` VRF:

```
switch# copy show-tech feature config sftp://root@10.0.0.1/tech.txt vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# copy show-tech local-file

`copy show-tech local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL> }`

## Description

Copies show tech output stored in a local file.

| Parameter                                                                       | Description                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>{&lt;REMOTE-URL&gt; [vrf &lt;VRF-NAME&gt;]   &lt;STORAGE-URL&gt; }</code> | Select either the remote URL or the storage URL for the destination of the copied command output. Required.                                                                                                                                                                                                                     |
| <code>&lt;REMOTE-URL&gt;</code>                                                 | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"><li>▪ <code>{tftp://}&lt;IP&gt;   &lt;HOST&gt;[:&lt;PORT&gt;] [&lt;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</code></li><li>▪ <code>{sftp://   scp:// &lt;USER&gt;@}&lt;IP&gt;   &lt;HOST&gt;[:&lt;PORT&gt;]/&lt;FILE&gt;</code></li></ul> |
| <code>vrf &lt;VRF-NAME&gt;</code>                                               | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                              |
| <code>&lt;STORAGE-URL&gt;</code>                                                | Specifies the USB to copy command output.<br>Syntax: <code>{usb}/&lt;FILE&gt;</code>                                                                                                                                                                                                                                            |

## Usage

Before entering the **copy show-tech local-file** command, run the **show tech** command with the **local-file** parameter for the specified feature.

## Examples

Copying the output to a remote URL:

```
switch# copy show-tech local-file tftp://10.100.0.12/file.txt
```

Copying the output to a remote URL:

```
switch# copy show-tech local-file scp://user@10.100.0.12/file.txt
```

Copying the output to a remote URL with a VRF:

```
switch# copy show-tech local-file tftp://10.100.0.12/file.txt vrf mgmt
```

Copying the output to a USB:

```
switch# copy show-tech local-file usb:/file
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy startup-config

```
copy startup-config {<STORAGE-URL> | <REMOTE-URL>}/config <CONFIG-NAME> [vrf <VRF-NAME>]
```

## Description

Copies the running configuration using TFTP, SFTP, SCP, or USB.

| Parameter                      | Description                                                                                                 |
|--------------------------------|-------------------------------------------------------------------------------------------------------------|
| {<STORAGE-URL>   <REMOTE-URL>} | Select either the storage URL or the remote URL for the destination of the copied command output. Required. |
| <STORAGE-URL>                  | Specifies the USB to copy command output.                                                                   |



| Parameter            | Description                                                                                                                                                                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Syntax:<br><b>{usb}:/&lt;FILE&gt;</b>                                                                                                                                                                                                                                                                                     |
| <REMOTE-URL>         | Specifies the URL to copy the command output.<br>Syntax:<br><ul style="list-style-type: none"> <li>▪ <b>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;][;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</b></li> <li>▪ <b>{sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</b></li> </ul> |
| config <CONFIG-NAME> | Specifies the startup configuration.                                                                                                                                                                                                                                                                                      |
| vrf <VRF-NAME>       | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                        |

## Examples

Copying the startup configuration to a remote URL:

```
switch# copy startup-config scp://root@10.0.1.1/config json vrf mgmt
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                                  |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

## copy support-files

```
copy support-files
 <REMOTE-URL> [vrf <VRF-NAME>]
 <STORAGE-URL>
all <REMOTE-URL> [vrf <VRF-NAME>]
all <STORAGE-URL>
feature <FEATURE-NAME> <STORAGE-URL>
previous-boot <REMOTE-URL> [vrf <VRF-NAME>]
previous-boot <STORAGE-URL>
```

## Description

Copies a set of support files to a compressed file in tar.gz format using TFTP, SFTP, SCP, or USB or to a directory over SFTP, USB, or local.



Do not press **Control + Z** at the password prompt while copying support files, as this will prevent the console from executing other commands.

| Parameter                                                                       | Description                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;FEATURE-NAME&gt;</code>                                               | The feature name, for example, <code>aaa</code> .                                                                                                                                                                                                                                                                               |
| <code>{&lt;REMOTE-URL&gt; [vrf &lt;VRF-NAME&gt;]   &lt;STORAGE-URL&gt; }</code> | Select either the remote URL or the storage URL for the destination of the copied command output. Required.                                                                                                                                                                                                                     |
| <code>&lt;REMOTE-URL&gt;</code>                                                 | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"><li>▪ <code>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;] [;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</code></li><li>▪ <code>{sftp://   scp://&lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}[:&lt;PORT&gt;]/&lt;FILE&gt;</code></li></ul> |
| <code>vrf &lt;VRF-NAME&gt;</code>                                               | Specifies the VRF name. The default VRF name is default. Optional.                                                                                                                                                                                                                                                              |
| <code>&lt;STORAGE-URL&gt;</code>                                                | Specifies the USB to copy command output.<br>Syntax: <code>{usb}:/&lt;FILE&gt;</code>                                                                                                                                                                                                                                           |

## Usage

If feature name is not provided, the command collects generic system-specific support information. If a feature name is provided, the command collects feature-specific support information.

## Examples

Copying the support files to a remote URL:

```
switch# copy support-files tftp://10.100.0.12/file.tar.gz
```

Copying the support files of the **lldp** feature to a remote URL with a specified VRF:

```
switch# copy support-files feature lldp tftp://10.100.0.12/file.tar.gz vrf mgmt
```

Copying the support files from the previous boot to a remote URL with a specified VRF:

```
switch# copy support-files previous-boot scp://user@10.0.14.206/file.tar.gz vrf mgmt
```

Copying the support files to a USB:

```
switch# copy support-files usb:/file.tar.gz
```

Copying all the support files to a remote URL:

```
switch# copy support-files all sftp://root@10.0.14.216/file.tar.gz vrf mgmt
```

Copying the support files of the **config** feature to a USB:

```
switch# copy support-files feature config usb:/file.tar.gz
```



Copying support files as a directory will not be allowed when system memory is insufficient. In the event this type of copy operation is attempted with low system memory, the command-line interface may display the error message: **Failed to collect support files due to insufficient system memory.**



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy support-files local-file

```
copy support-files [feature <FEATURE-NAME> | previous-boot | all] local-file {<REMOTE-URL> [vrf <VRF-NAME>] | <STORAGE-URL>}
```

## Description

Stores a set of support files as a compressed file in the switch locally and copies the preserved support files to a directory using TFTP, SFTP, SCP, USB, or local. . You can store only one copy of the support file locally. When you store a new support file, it overwrites the existing support file



Do not press **Control + Z** at the password prompt while copying support files, as this will prevent the console from executing other commands.

| Parameter      | Description                                                                                    |
|----------------|------------------------------------------------------------------------------------------------|
| <FEATURE-NAME> | Specifies the feature for the support files.                                                   |
| <SLOT-ID>      | Specifies the module slot number identifier for the support files.<br>Range: 1/1-1/4, 1/7-1/10 |
| <MEMBER-ID>    | Specifies the VSF member identifier for the support files. Range: 1-10                         |
| <REMOTE-URL>   | Specifies the URL to copy the support files.                                                   |
| <STORAGE-URL>  | Specifies the USB to copy the support files.                                                   |
| <VRF-NAME>     | Specifies the VRF name. The default VRF name is default.                                       |

## Usage

If the copy of the support files to the destination fails, an alternate option is prompted to store the collected data in the local file. This helps us to retry the copy process using **copy support-files local-file** <REMOTE-URL/STORAGE-URL> without the need of regenerating the file.

## Examples

Copying support file to the local file:

```
switch# copy support-files local-file
switch# copy support-files feature lldp local-file
switch# copy support-files previous-boot local-file
switch# copy support-files all local-file
The operation to copy all support files could take a while to complete.
Do you want to continue (y/n)?
```

Copying local support file to a remote URL and storage URL:

```
switch# copy support-files local-file usb:/support_files_dir_path/
switch# copy support-files local-file scp://root@10.0.14.206//support_files_dir_
path/abc.tar.gz vrf mgmt
```



Copying support files as a directory will not be allowed when system memory is insufficient. In the event this type of copy operation is attempted with low system memory, the command-line interface may display the error message: **Failed to collect support files due to insufficient system memory.**



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## copy support-log

### Description

Copies the specified support log for a daemon TFTP, SFTP, SCP, USB, or local.

| Parameter                                                                      | Description                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;DAEMON-NAME&gt;</code>                                               | Specifies the name of the daemon. Required.                                                                                                                                                                                                                                                                         |
| <code>{&lt;STORAGE-URL&gt;   &lt;REMOTE-URL&gt; [vrf &lt;VRF-NAME&gt;]}</code> | Selects either the storage URL or the remote URL for the destination of the copied command output. Required.                                                                                                                                                                                                        |
| <code>&lt;STORAGE-URL&gt;</code>                                               | Specifies the USB to copy command output.<br>Syntax: <b>{usb}:/&lt;FILE&gt;</b>                                                                                                                                                                                                                                     |
| <code>&lt;REMOTE-URL&gt;</code>                                                | Specifies the URL to copy the command output.<br>Syntax: <ul style="list-style-type: none"><li>▪ <b>{tftp://}{&lt;IP&gt;   &lt;HOST&gt;}:{&lt;PORT&gt;}[;blocksize=&lt;VAL&gt;]/&lt;FILE&gt;</b></li><li>▪ <b>{sftp://   scp:// &lt;USER&gt;@}{&lt;IP&gt;   &lt;HOST&gt;}:{&lt;PORT&gt;}/&lt;FILE&gt;</b></li></ul> |
| <code>vrf &lt;VRF-NAME&gt;</code>                                              | Specifies the VRF name. If no VRF name is provided, the VRF named <i>default</i> is used. Optional.                                                                                                                                                                                                                 |

### Usage

Fast log is a high performance, per-daemon binary logging infrastructure used to debug daemon level issues by precisely capturing the per daemon/module/functionalities debug traces in real time. Fast log, also referred to as support logs, helps users to understand the feature internals and its specific happenings. The fast logs from one daemon are not overwritten by other daemon logs because fast logs are captured as part of a daemon core dump. Fast logs are enabled by default.

### Examples

Copying the support log from the daemon hpe-fand to a remote URL:

```
switch# copy support-log hpe-fand tftp://10.100.0.12/file
```

Copying the support log from the daemon fand to a remote URL with a VRF named mgmt:

```
switch# copy support-log fand scp://user@10.100.0.12/file vrf mgmt
```

Copying the support log from the daemon hpe-fand to a remote URL with a VRF named mgmt:

```
switch# copy support-log hpe-fand tftp://10.100.0.12/file vrf mgmt
```

Copying the support log from the daemon hpe-fand to a USB:

```
switch# copy support-log hpe-fand usb:/support-log
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification       |
|------------------|--------------------|
| 10.08            | Added SCP support. |
| 10.07 or earlier | --                 |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## allow-non-failsafe-updates

allow-non-failsafe-updates <num\_minutes>

### Description

Allow non-failsafe updates of programmable devices for the specified number of minutes, or **enter** 0 to disallow unsafe updates. The maximum permitted value is 120 minutes.

### Example

The following example will enable non-failsafe updates of programmable devices for the next 30 minutes.

```
switch(config)# allow-non-failsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes. You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin applying any
needed
updates. Ensure that the switch will not lose power, be rebooted again, or have
any
modules removed until all updates have finished and all line and fabric modules
have
returned to the ready state

WARNING: Interrupting these updates may make the product unusable!

Continue [y/n] ? y

Unsafe updates : allowed (less than 30 minute(s) remaining)
```



For more information on how to use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release    | Modification |
|------------|--------------|
| 10.15.1010 | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# bluetooth disable

bluetooth disable  
no bluetooth disable

## Description

Disables the Bluetooth feature on the switch. The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE). Bluetooth is enabled by default.

The **no** form of this command enables the Bluetooth feature on the switch.

## Example

Disabling Bluetooth on the switch. <XXXX> is the switch platform and <NNNNNNNNNN> is the device identifier.

```
switch(config)# bluetooth disable
switch# show bluetooth
Enabled : No
Device name : <XXXX>--<NNNNNNNNNN>

switch(config)# show running-config
...
bluetooth disabled
...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# bluetooth enable

bluetooth enable  
no bluetooth enable

## Description

This command enables the Bluetooth feature on the switch. The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE).

Default: Bluetooth is enabled by default.

The **no** form of this command disables the Bluetooth feature on the switch.



## Usage

The default configuration of the Bluetooth feature is `enabled`. The output of the `show running-config` command includes Bluetooth information only if the Bluetooth feature is disabled.

The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE).

The Bluetooth feature requires the USB feature to be enabled. If the USB feature has been disabled, you must enable the USB feature before you can enable the Bluetooth feature.

## Examples

```
switch(config)# bluetooth enable
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## clear events

```
clear events
```

### Description

Clears up event logs. Using the `show events` command will only display the logs generated after the `clear events` command.

### Examples

Clearing all generated event logs:

```
switch# show events

show event logs

2018-10-14:06:57:53.534384|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource
utilization poll interval is changed to 27
2018-10-14:06:58:30.805504|lldpd|103|LOG_INFO|MSTR|1|Configured LLDP tx-timer to
36
2018-10-14:07:01:01.577564|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource
utilization poll interval is changed to 49
```

```
switch# clear events

switch# show events

show event logs

2018-10-14:07:03:05.637544|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource
utilization poll interval is changed to 34
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## clear ip errors

```
clear ip errors
```

### Description

Clears all IP error statistics.

### Example

Clearing and showing ip errors:

```
switch# clear ip errors
switch# show ip errors

Drop reason Packets

Malformed packets 0
IP address errors 0
...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## console baud-rate

```
console baud-rate <SPEED>
no console baud-rate <SPEED>
```

### Description

Sets the console serial port speed.

The no form of this command resets the console port speed to its default of 115200 bps.

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| <SPEED>   | Selects the console port speed in bps, either 9600 or 115200. |

### Usage

The speed change occurs immediately for the active console session. The console will be inaccessible until the client terminal settings are updated to match the console port speed that you set. After the command is executed you will be prompted to log in again.

### Examples

Setting the console port speed to 9600 bps:

```
switch(config)# console baud-rate 9600
This command will configure the baud rate immediately for the active serial
console session. After the command is executed the user will be prompted to
re-login. The serial console will be inaccessible until the terminal client
settings are updated to match the baud rate of the switch.
Continue (y/n)? y
```

Resetting the console port to its default speed 115200 bps:

```
switch(config)# no console baud-rate
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## domain-name

```
domain-name <NAME>
no domain-name [<NAME>]
```

### Description

Specifies the domain name of the switch.

The **no** form of this command sets the domain name to the default, which is no domain name.

| Parameter | Description                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <NAME>    | Specifies the domain name to be assigned to the switch. The first character of the name must be a letter or a number. Length: 1 to 32 characters. |

### Examples

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Setting the domain name to the default value:

```
switch(config)# no domain-name
switch(config)# show domain-name

switch(config)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# hostname

```
hostname <HOSTNAME>
no hostname [<HOSTNAME>]
```

## Description

Sets the host name of the switch.

The **no** form of this command resets the host name to the default value `switch`.

| Parameter  | Description                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------|
| <HOSTNAME> | Specifies the host name. First and last characters must be alphanumeric. Maximum string length: 63. |

## Examples

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
myswitch
```

Setting the host name to the default value:

```
myswitch(config)# no hostname
switch(config)#
```

Error messages:

```
switch(config)# hostname
ThisIsAVeryLongHostnameThatExceedsTheMaximumLengthLimitOf64Characters
The hostname cannot exceed 63 characters in length.
switch(config)#
```

```
switch(config)# hostname -abd-123-
The hostname must begin and end with a letter or number.
switch(config)#
```

```
switch(config)# hostname abc.123@12
To be compliant with RFC 1123, the hostname must contain only letters, numbers and
hyphens, and must not start or end with a hyphen.
switch(config)#
```

```
switch(config)# hostname 123_123
Hostname contains one or more non-RFC 1123 compliant characters. Some features may
not work as intended.
Do you want to continue (y/n)? y
123_123(config)#
```

```
switch(config)# hostname test.name
Hostname contains one or more non-RFC 1123 compliant characters. Some features may
not work as intended.
Do you want to continue (y/n)? y
test.name(config)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                               |
|------------------|----------------------------------------------------------------------------|
| 10.17            | Enhanced <b>hostname</b> to support dot (.) and underscore (_) characters. |
| 10.07 or earlier | --                                                                         |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## led locator

```
led locator
on
off
flashing
slow_blink
fast_blink
half_bright
no...
```

## Description

Sets the state of the locator LED.

| Parameter   | Description                                    |
|-------------|------------------------------------------------|
| on          | Turns on the LED.                              |
| off         | Turns off the LED, which is the default value. |
| flashing    | Sets the LED to blink on and off repeatedly.   |
| slow_blink  | Sets the LED to slow blink on and off.         |
| fast_blink  | Sets the LED to fast blink on and off.         |
| half_bright | Sets the LED intensity to half bright.         |
| no          | Negates any configured parameter               |

## Example

Setting the state of the locator LED:

```
switch# led locator flashing
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                                                                                   |
|------------------|--------------------------------------------------------------------------------------------------------------------------------|
| 10.13            | Starting with AOS-CX 10.13, this command will not take effect when it is sent to the switch from HPE Aruba Networking Central. |
| 10.07 or earlier | --                                                                                                                             |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## mtrace

```
mtrace <IPV4-SRC-ADDR> <IPV4-GROUP-ADDR> [lhr <IPV4-LHR-ADDR>] [ttl <HOPS>]
[vrf <VRF-NAME>]
```

## Description

Traces the specified IPv4 source and group addresses.

| Parameter                    | Description                                                                             |
|------------------------------|-----------------------------------------------------------------------------------------|
| <i>IPV4-SRC-ADDR</i>         | Specifies the source IPv4 address to trace.                                             |
| <i>IPV4-GROUP-ADDR</i>       | Specifies the group IPv4 address to trace.                                              |
| lhr < <i>IPV4-LHR-ADDR</i> > | Specifies the last hop router address from which to start the trace.                    |
| ttl < <i>HOPS</i> >          | Specifies the Time-To-Live duration in hops. Range: 1 to 255 hops. Default: 8 hops.     |
| vrf < <i>VRF-NAME</i> >      | Specifies the name of the VRF. If a name is not specified the default VRF will be used. |

## Examples

Tracing with source, group, and LHR addresses and TTL:

```
(switch)# mtrace 20.0.0.1 239.1.1.1 lhr 10.1.1.1 ttl 10

Type escape sequence to abort.
Mtrace from 10.0.0.1 for Source 20.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0 10.0.0.1
-1 30.0.0.1 PIM 0 ms
-2 40.0.0.1 PIM 2 ms
-3 50.0.0.1 PIM 100 ms
-4 60.0.0.1 PIM 156 ms
-5 20.0.0.1 PIM 123 ms
```

Tracing with source and group addresses:

```
(switch)# mtrace 200.0.0.1 239.1.1.1

Type escape sequence to abort.
Mtrace from self for Source 200.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0 10.0.0.1
-1 30.0.0.1 PIM 0 ms
-2 40.0.0.1 PIM 2 ms
-3 50.0.0.1 PIM 100 ms
-4 60.0.0.1 PIM 156 ms
-5 200.0.0.1 PIM 123 ms
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |



## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## power consumption-average-period

power consumption-average-period <PERIOD-IN-SECONDS>

### Description

Configures a time period for average power consumption in seconds.

| Parameter           | Description                                                                              |
|---------------------|------------------------------------------------------------------------------------------|
| <PERIOD-IN-SECONDS> | Specifies the period in seconds for average power consumed. Range: 60-3600. Default: 600 |

### Example

Configuring a time period of 60 seconds for average power consumption:

```
switch(config)# power consumption-average-period 60
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.13   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## show bluetooth

show bluetooth

### Description

Shows general status information about the Bluetooth wireless management feature on the switch.

### Usage

This command shows status information about the following:

- The USB Bluetooth adapter
- Clients connected using Bluetooth
- The switch Bluetooth feature.

The output of the **show running-config** command includes Bluetooth information only if the Bluetooth feature is disabled.

The device name given to the switch includes the switch serial number to uniquely identify the switch while pairing with a mobile device.

The management IP address is a private network address created for managing the switch through a Bluetooth connection.

## Examples

Example output when Bluetooth is enabled but no Bluetooth adapter is connected. <XXXX> is the switch platform and <NNNNNNNNNN> is the device identifier.

```
switch# show bluetooth
Enabled : Yes
Device name : <XXXX>-<NNNNNNNNNN>
Adapter State : Absent
```

Example output when Bluetooth is enabled and there is a Bluetooth adapter connected:

```
switch# show bluetooth
Enabled : Yes
Device name : <XXXX>-
Adapter State : Ready
Adapter IP address : 192.168.99.1
Adapter MAC address : 480fcf-af153a

Connected Clients

Name MAC Address IP Address Connected Since

Mark's iPhone 089734-b12000 192.168.99.10 2018-07-09 08:47:22 PDT
```

Example output when Bluetooth is disabled:

```
switch# show bluetooth
Enabled : No
Device name : <XXXX>-<NNNNNNNNNN>
```



---

For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show boot-history

```
show boot-history [all|{vsf member <1-10>}]
```

### Description

Shows boot history information. When no parameters are specified, shows the most recent information about the current boot operation, and the three previous boot operations for the switch. When the **all** parameter is specified, the output of this command shows the boot information for the active management module.

.



To view boot-history on a standby, the command must be sent on the conductor console.

| Parameter         | Description                                                        |
|-------------------|--------------------------------------------------------------------|
| all               | Optional. Shows boot information for the active management module. |
| vsf member <1-10> | Optional. Display boot history for the specified VSF member        |

### Usage

This command displays the boot-index, boot-ID, and up time in seconds for the current boot. If there is a previous boot, it displays boot-index, boot-ID, reboot time (based on the time zone configured in the system) and reboot reasons. Previous boot information is displayed in reverse chronological order.

The output of this command includes the following information:

| Parameter                   | Description                                                                                                                                 |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Index                       | The position of the boot in the history file. Range: 0 to 3.                                                                                |
| Boot ID                     | A unique ID for the boot . A system-generated 128-bit string.                                                                               |
| Current Boot, up for <time> | For the current boot, the <b>show boot-history</b> command shows the number of seconds the module has been running on the current software. |

| Parameter                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <Timestamp>: boot reason | <p>For previous boot operations, the <b>show boot-history</b> command shows the time at which the operation occurred and the reason for the boot. The reason for the boot is one of the following values:</p> <ul style="list-style-type: none"> <li>▪ <b>&lt;DAEMON-NAME&gt; crash:</b> The daemon identified by &lt;DAEMON-NAME&gt; caused the module to boot.</li> <li>▪ <b>Kernel crash:</b> The operating system software associated with the module caused the module to boot.</li> <li>▪ <b>Uncontrolled reboot:</b> The reason for the reboot is not known.</li> <li>▪ <b>Reboot requested through database:</b> The reboot occurred because of a request made through the CLI or other API.</li> </ul> |

## Examples

Showing the boot history of the active management module:

```
switch# show boot-history
Management module
=====

Index : 2
Boot ID : c34a2c2499004a02bbeeff4992e1fdbd
Current Boot, up for 1 days 13 hrs 13 mins 27 secs

Index : 1
Boot ID : bfba9bc486304e57904ac717a0ccbdcd
02 Sep 23 02:55:33 : CPU request reset with 0x20201, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:55:33 : Switch boot count is 2

Index : 0
Boot ID : a88a71b7ca9a4574af7e3b811ddfdc7e
02 Sep 23 02:49:26 : Reboot requested by user, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:50:02 : Switch boot count is 1

Index : 3
Boot ID : f00ba10c8c44457f83fee303d014a89a
25 Aug 23 10:27:42 : Power on reset with 0x1, Version: FL.10.14.0000-1465-
g9df95249d06b0~dirty
25 Aug 23 10:28:18 : Switch boot count is 3
25 Aug 23 10:29:02 : Primary overtemperature fault detected with 0x2 in PSU 1/1
```

Showing the boot history of the active management module and all line modules:



For more information on features that use this command, refer to the Fundamentals Guide or the Monitoring Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show capacities

`show capacities <FEATURE> [vsx-peer]`

### Description

Shows system capacities and their values for all features or a specific feature.

| Parameter                    | Description                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;FEATURE&gt;</code> | Specifies a feature. For example, <b>aaa</b> or <b>vrrp</b> .                                                                                                                                                                    |
| <code>vsx-peer</code>        | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Usage

Capacities are expressed in user-understandable terms. Thus they may not map to a specific hardware or software resource or component. They are not intended to define a feature exhaustively.

### Examples

Showing all available capacities for BGP:

```
switch# show capacities bgp

System Capacities: Filter BGP
Capacities Name Value

-
Maximum number of AS numbers in as-path attribute
32
...
```

Showing all available capacities for mirroring:

```
switch# show capacities mirroring

System Capacities: Filter Mirroring
Capacities Name Value

```

```
-
Maximum number of Mirror Sessions configurable in a system
4
Maximum number of enabled Mirror Sessions in a system
4
```

Showing all available capacities for MSTP:

```
switch# show capacities mstp

System Capacities: Filter MSTP
Capacities Name Value

-
Maximum number of mstp instances configurable in a system
64
```

Showing all available capacities for VLAN count:

```
switch# show capacities vlan-count

System Capacities: Filter VLAN Count
Capacities Name Value

-
Maximum number of VLANs supported in the system
4094
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show capacities-status

```
show capacities-status <FEATURE> [vsx-peer]
```

### Description

Shows system capacities status and their values for all features or a specific feature.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <FEATURE> | Specifies the feature, for example <b>aaa</b> or <b>vrrp</b> for which to display capacities, values, and status. Required.                                                                                                      |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing the system capacities status for all features:

```
switch# show capacities-status

System Capacities Status
Capacities Status Name Value Maximum

Number of active gateway mac addresses in a system 0 16
Number of aspath-lists configured 0 64
Number of community-lists configured 0 64
...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show console

show console

### Description

Shows the serial console port current speed.

### Examples

Showing the console port current speed:

```
switch# show console
Baud Rate: 9600
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show core-dump

```
show core-dump all
```

## Description

Shows core dump information about the specified module. When no parameters are specified, shows only the core dumps generated in the current boot of the management module. When the **all** parameter is specified, shows all available core dumps.

| Parameter | Description                     |
|-----------|---------------------------------|
| all       | Shows all available core dumps. |

## Usage

When no parameters are specified, the **show core-dump** command shows only the core dumps generated in the current boot of the management module. You can use this command to determine when any crashes are occurring in the current boot.

If no core dumps have occurred, the following message is displayed: **No core dumps are present**

To show core dump information for the standby management module, you must use the **standby** command to switch to the standby management module and then execute the **show core-dump** command.

In the output, the meaning of the information is the following:

Daemon Name

Identifies name of the daemon for which there is dump information.

Instance ID

Identifies the specific instance of the daemon shown in the **Daemon Name** column.

Present

Indicates the status of the core dump:

Yes



The core dump has completed and available for copying.

In Progress

Core dump generation is in progress. Do not attempt to copy this core dump.

Timestamp

Indicates the time the daemon crash occurred. The time is the local time using the time zone configured on the switch.

Build ID

Identifies additional information about the software image associated with the daemon.

## Examples

Showing core dump information for the current boot of the active management module only:

```
switch# show core-dump
=====
Daemon Name | Instance ID | Present | Timestamp | Build ID
=====
hpe-fand 1399 Yes 2017-08-04 19:05:34 1246d2a
hpe-sysmond 957 Yes 2017-08-04 19:05:29 1246d2a
=====
Total number of core dumps : 2
=====

=====
Daemon Name | Instance ID | Present | Timestamp | Build ID
=====
hpe-fand 1399 Yes 2017-08-04 19:05:34 1246d2a
hpe-sysmond 957 Yes 2017-08-04 19:05:29 1246d2a
=====
Total number of core dumps : 2
=====
```

Showing all core dumps:

```
switch# show core-dump all
=====
Management Module core-dumps
=====
Daemon Name | Instance ID | Present | Timestamp | Build ID
=====
hpe-sysmond 513 Yes 2017-07-31 13:58:05 e70f101
hpe-tempd 1048 Yes 2017-08-13 13:31:53 e70f101
hpe-tempd 1052 Yes 2017-08-13 13:41:44 e70f101
=====
Line Module core-dumps
=====
Line Module : 1/1
=====
dune_agent_0 18958 Yes 2017-08-12 11:50:17 e70f101
dune_agent_0 18842 Yes 2017-08-12 11:50:09 e70f101
=====
Total number of core dumps : 5
=====
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show deprecated commands

`show deprecated-commands [<feature>]`

### Description

Shows the list of CLI commands that will be deprecated in a future release along with the new form of the same command which is recommended for use.

Both the command options will be supported until a certain release, after which only the newer replacement command will be supported.

| Parameter            | Description                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------|
| <code>feature</code> | Optional.<br>Specify feature name.<br>The list of features for which you can view deprecated commands are: |

### Examples

Check the deprecated CLI commands for a specific feature:

```
switch# show deprecated-commands

The following commands with ipv4 keyword will be replaced with ip

Deprecated: vrrp <1-255> address-family (ipv4 | ipv6)
Replacement: vrrp <1-255> address-family (ip | ipv6)

Deprecated: show bgp ipv4 unicast
Replacement: show bgp ip unicast
...

switch# show deprecated-commands vrrp

The following commands with ipv4 keyword will be replaced with ip

Deprecated: vrrp <1-255> address-family (ipv4 | ipv6)
Replacement: vrrp <1-255> address-family (ip | ipv6)
```

```
Deprecated: show vrrp (ipv4 | ipv6 | brief | detail) (<1-255>)
Replacement: show vrrp (ip | ipv6 | brief | detail) (<1-255>)
...

switch# show deprecated-commands vsf
Feature vsf has no deprecated commands.
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.14   | Command introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show domain-name

```
show domain-name [vsx-peer]
```

### Description

Shows the current domain name.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Usage

If there is no domain name configured, the CLI displays a blank line.

### Example

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
```

```
switch(config)# show domain-name
example.com
switch(config)#
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show environment fan

```
show environment fan [vsx-peer]
```

## Description

Shows the status information for all fans and fan trays (if present) in the system.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Usage

For fan trays, **Status** is one of the following values:

- ready:The fan tray is operating normally.
- fault:The fan tray is in a fault event. The status of the fan tray does not indicate the status of fans.
- empty:The fan tray is not installed in the system.

For fans:

Speed :Indicates the relative speed of the fan based on the nominal speed range of the fan. Values are:

Slow:The fan is running at less than 25% of its maximum speed.

Normal:The fan is running at 25-49% of its maximum speed.

Medium:The fan is running at 50-74% of its maximum speed.

Fast:The fan is running at 75-99% of its maximum speed.

Max:The fan is running at 100% of its maximum speed.

N/A:The fan is not installed.

Direction: The direction of airflow through the fan. Values are:

front-to-back:Air flows from the front of the system to the back of the system.  
N/A:The fan is not installed.  
Status: Fan status. Values are:  
**uninitialized**:The fan has not completed initialization.  
**ok**: The fan is operating normally.  
**fault**: The fan is in a fault state.  
**empty**: The fan is not installed.

## Examples

Showing output for a system without a fan tray:

```
switch# show environment fan

Fan information

Fan Serial Number Speed Direction Status RPM

1 SGXXXXXXXXXX slow front-to-back ok 6000
2 SGXXXXXXXXXX normal front-to-back ok 8000
3 SGXXXXXXXXXX medium front-to-back ok 11000
4 SGXXXXXXXXXX fast front-to-back ok 14000
5 SGXXXXXXXXXX max front-to-back fault 16500
6 N/A N/A N/A empty
...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show environment led

```
show environment led [vsx-peer]
```

### Description

Shows state and status information for all the configurable LEDs in the system.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vsx-peer</code> | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

Showing state and status for LED:



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show environment power-consumption

```
show environment power-consumption [detail]
```

## Description

Displays power consumption information.

| Parameter                      | Description                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <code>[detail]</code>          | Displays detailed power consumption information.                                                                        |
| <code>&lt;MEMBER-ID&gt;</code> | For VSF supported platforms only. Displays the power consumption information for the specified VSF member. Range: 1-10. |

## Usage

Power consumed values are updated every 5 seconds. The total power consumed is the total power used in a chassis. The power consumed average is calculated from the total power consumed as a running average over a period of time. The average period has a default of 10 minutes. The period can be configured using **power-consumption-average-period**.

On chassis where power input is not supported, power consumed is displayed as Power Usage and PSU Output Power is displayed as N/A.

The following information is provided for a summary of power consumption:

- line module: power used by line module
- management module: power used by management module
- fabric module: power used by fabric module
- chassis module: power used by chassis module
- fan module: power used by fan module
- power total: total power consumption
- average power: average for total power consumption that is calculated over a given period
- average period: time to calculate power average

For more information, see the video [AOS-CX 10.14 Release Update: Sustainability Update](#).

## Example

Showing the power consumption for a 1RU switch:

```
switch# show environment power-consumption

Power Consumption Averaging Period : 600 seconds
```

| Name | Description          | Power Usage (W) |         | PSU Output (W) |         |
|------|----------------------|-----------------|---------|----------------|---------|
|      |                      | Instant         | Average | Instant        | Average |
| 1    | 8360-32Y4C v2 Switch | 120.00          | 111.16  | 111.00         | 102.62  |

Showing the power consumption for a VSF stack:

```
switch# show environment power-consumption

Power Consumption Averaging Period : 600 seconds
```

| Name | Description        | Power Usage (W) |         | PSU Output (W) |         |
|------|--------------------|-----------------|---------|----------------|---------|
|      |                    | Instant         | Average | Instant        | Average |
| 1    | 6200M 24G 4SFP+ Sw | 350.00          | 349.62  | 300.00         | 311.50  |
| 2    | 6200M 24G 4SFP+ Sw | 300.00          | 299.50  | 280.00         | 275.50  |

Showing the power consumption for a switch where input reading is not supported:

```
switch# show environment power-consumption

Power Consumption Averaging Period : 600 seconds
```

| Name | Description        | Power Usage (W) |         | PSU Output (W) |         |
|------|--------------------|-----------------|---------|----------------|---------|
|      |                    | Instant         | Average | Instant        | Average |
| 1    | 6200M 24G 4SFP+ Sw | 321.00          | 330.30  | N/A            | N/A     |

Showing the power consumption for a switch with multiple line cards, in brief:

```
switch# show environment power-consumption
Power Consumption Averaging Period : 600 seconds
```

| Name | Description     | Power Usage (W) |         | PSU Output (W) |         |
|------|-----------------|-----------------|---------|----------------|---------|
|      |                 | Instant         | Average | Instant        | Average |
| 1    | 6410 v2 Chassis | 900.00          | 905.62  | 798.00         | 803.23  |

Showing the power consumption for a switch with multiple line cards, in detail:

```
switch# show environment power-consumption detail
Power Consumption Averaging Period : 600 seconds
```

| Name | Module     | Type  | Power Usage (W) |         | PSU Output (W) |         |
|------|------------|-------|-----------------|---------|----------------|---------|
|      |            |       | Instant         | Average | Instant        | Average |
| 1    | chassis    | total | 1495.00         | 1499.99 | 1307.00        | 1300.67 |
| 1/3  | line       |       | 97.00           |         |                |         |
| 1/4  | line       |       | 95.00           |         |                |         |
| 1/5  | line       |       | 90.00           |         |                |         |
| 1/6  | line       |       | 58.00           |         |                |         |
| 1/7  | line       |       | 90.00           |         |                |         |
| 1/8  | line       |       | 93.00           |         |                |         |
| 1/9  | line       |       | 96.00           |         |                |         |
| 1/10 | line       |       | 92.00           |         |                |         |
| 1/11 | line       |       | 100.00          |         |                |         |
| 1/12 | line       |       | 99.00           |         |                |         |
| 1/1  | management |       | 14.00           |         |                |         |
| 1/2  | management |       | 13.00           |         |                |         |
|      | other      |       | 370.00          |         |                |         |

Showing the power consumption for 4 member stack, in detail:

```
switch# show environment power-consumption detail
Power Consumption Averaging Period : 600 seconds
```

| Name | Module  | Type  | Power Usage (W) |         | PSU Output (W) |         |
|------|---------|-------|-----------------|---------|----------------|---------|
|      |         |       | Instant         | Average | Instant        | Average |
| 1    | chassis | total | 930.00          | 905.17  | 830.00         | 803.40  |
| 2    | chassis | total | 900.00          | 920.00  | 875.00         | 880.25  |
| 3    | chassis | total | 850.00          | 857.25  | 802.00         | 805.00  |
| 4    | chassis | total | 1200.00         | 1100.56 | 921.00         | 950.00  |

```
Total Power Consumption 3428.00
```

Showing the power consumption for VSF member 2:

```
switch# show environment power-consumption member 2
```

```
Power Consumption Averaging Period : 600 seconds
```

| Name | Description        | Power Usage (W) |         | PSU Output (W) |         |
|------|--------------------|-----------------|---------|----------------|---------|
|      |                    | Instant         | Average | Instant        | Average |
| 2    | 6200M 24G 4SFP+ Sw | 300.00          | 299.50  | 280.00         | 275.50  |

Showing the power consumption for VSF invalid member:



```
switch# show environment power-consumption member 5
Member 5 is not present
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release    | Modification                                                               |
|------------|----------------------------------------------------------------------------|
| 10.14.1000 | Introduced enhancement to power consumption and power consumption average. |
| 10.13      | Command introduced.                                                        |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

# show environment power-supply

```
show environment power-supply
 input-voltage [events] [vsf member <MEMBER-ID>]
 vsx-peer
```

## Description

Shows status information about all power supplies in the switch.

| Parameter     | Description                                                                                                                                                                                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| input-voltage | Display the statistic and status of the Power Supply Unit (PSU) input voltage. This parameter is supported on 5420, 6200M, 6300M, 6400, 8320, 8325/8325H/8325P, 8100, 8360, 8400, 9300/9300S and 10000 Switch series.                                |
| events        | Include the optional <b>events</b> parameter to display events for the power supply's input voltage. the output of the command displays information for the power supplies of the entire chassis or system (including the PSUs within a VSF member.) |
| vsx-peer      | Shows the output from the VSX peer switch. This parameter is only available on switches with profiles that support VSX. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed.  |

## Usage

The following information is provided for each power supply:

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mbr/PSU         | Shows the member and slot number of the power supply.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Product Number  | Shows the product number of the power supply.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Serial Number   | Shows the serial number of the power supply, which uniquely identifies the power supply.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| PSU Status      | <p>The status of the power supply. Values are:</p> <p>Here is your list with the numbers removed:</p> <ul style="list-style-type: none"> <li>▪ <b>OK:</b> power supply is operating normally</li> <li>▪ <b>OK*:</b> power supply is operating normally, although there is insufficient power to fully power the chassis.</li> <li>▪ <b>Empty:</b> no power supply is installed</li> <li>▪ <b>Absent:</b> no power supply in installed when one is expected</li> <li>▪ <b>Input Fault:</b> there is a fault condition on the input of the power supply</li> <li>▪ <b>Output Fault:</b> there is a fault condition on the output of the power supply</li> <li>▪ <b>PoE Fault:</b> there is a fault condition on the PoE output of the power supply</li> <li>▪ <b>Airflow Fault:</b> airflow direction does not match the expected chassis airflow direction</li> <li>▪ <b>Redundancy Fault:</b> type of capacity does not match the expected redundancy type and capacity</li> <li>▪ <b>Mixed Input Fault:</b> the input type of the inserted power supplies does not match. AC and DC power supplies cannot be mixed in the same switch.</li> <li>▪ <b>Warning:</b> there is an internal fault condition but the power supply is still operational</li> <li>▪ <b>Non-recoverable Fault:</b> there is an internal fault condition that the power supply cannot recover from</li> <li>▪ <b>Unsupported:</b> power supply is not of a known supported type</li> <li>▪ <b>Unknown:</b> power supply has experienced an unknown fault condition</li> <li>▪ <b>Alert:</b> power supply has experienced an abnormal event but is still operational</li> <li>▪ <b>Undervoltage:</b> Power supply's input voltage dips below the minimum operating voltage</li> </ul> |
| input type      | Power supply's input type Identification. It can be <b>AC</b> or <b>DC</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Voltage Range   | Valid operating voltage range for the power supply to support the current wattage maximum.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Wattage Maximum | Maximum amount of wattage that the power supply can provide                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

If you include the optional **input-voltage** parameter, the output includes the following information:

| Output Column    | Description                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------|
| Mbr/PSU          | Shows the member and slot number of the power supply.                                                            |
| Product Number   | Shows the product number of the power supply.                                                                    |
| Input Type       | Power supply's input type Identification. It can be <b>AC</b> or <b>DC</b> .                                     |
| Normal Input (V) | Normal operating voltage range for the power supply to support current wattage maximum - according to regulatory |

| Output Column                               | Description                                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------|
|                                             | requirements.                                                                                                |
| Present Input (V)                           | Instantaneous input voltage reading acquired from power supply                                               |
| Average Input                               | The average input voltage over the last 15 minutes (or since power was applied if less than 15 minutes ago). |
| Input voltage Violations: Count             | Number of occurrences for which PSU's input voltage crosses outside of the normal input.                     |
| Input voltage Violations: Most Recent Event | Timestamp of the most recent violation where the PSU input voltage crosses outside of the normal input.      |
| Recovery Count                              | Number of occurrences when the PSU's input voltage recovers to within the normal input range.                |
| Recovery Time                               | Timestamp of the most recent input voltage's recovery.                                                       |

## Examples

Showing example output when only one power supply is installed in a switch that supports modular power supplies:

```
switch# show environment power-supply
```

| Mbr/PSU | Product Number | Serial Number | PSU Status | Input Type | Voltage Range | Wattage Maximum |
|---------|----------------|---------------|------------|------------|---------------|-----------------|
| 1/1     | JL670A         | CN97KN803F    | OK         | AC         | 200V-240V     | 1600            |
| 1/2     | N/A            | N/A           | Absent     | --         | --            | 0               |

The output of the following command shows input voltage data for a power supply. In the following example, the output of the **show environment power-supply input-voltage** command has been broken into two sections to better fit in this document. In the product command-line interface, the output appears as a single, wide table.

```
switch# show environment power-supply input-voltage
```

Input Voltage Averaging Period : 15 minutes

| Mbr/PSU | Product Number | Input Type | Normal Input (V) | Present Input (V) | Average Input (V) | Input Voltage Violations Count |
|---------|----------------|------------|------------------|-------------------|-------------------|--------------------------------|
| 1/1     | JL670A         | AC         | 180-264          | 231.7             | 231.2             | 1                              |
| 1/2     | JL670A         | AC         | 180-264          | --                | --                | 0                              |

| Most Recent Event            | Recovery Count | Recovery Time                |
|------------------------------|----------------|------------------------------|
| Mon Jun 23 02:45:28 UTC 2025 | 1              | Mon Jun 23 02:45:41 UTC 2025 |
| N/A                          | 0              | N/A                          |

Showing individual input voltage events for a switch power supply:

```
switch# show environment power-supply input-voltage events

Mbr/PSU : 1/2
Product Number : JL758A
Serial Number : CN1AL6H326
Status : OK
Input Type : DC
Normal Input (V) : 40-60
Present Input : 44.8 V
Average Input : 43.1 V
Averaging Period : 15 minutes
Max Input : 48.9 V
Min Input : 36.9 V
ID Type Voltage Timestamp

0 violation 37.8 Mon Jul 21 06:37:53 UTC 2025
1 recovered 40.1 Mon Jul 21 09:01:44 UTC 2025

Mbr/PSU : 1/2
Product Number : JL670A
Serial Number : CN1AL6H326
Status : OK
Input Type : AC
Normal Input (V) : 99-140
Present Input : 100.8 V
Average Input : 104.2 V
Averaging Period : 15 minutes
Max Input : 119.8 V
Min Input : 95.5 V
ID Type Voltage Timestamp

0 violation 96.5 Wed Jul 02 08:51:07 UTC 2025
1 recovered 99.1 Wed Jul 02 08:54:55 UTC 2025
2 violation 96.6 Wed Jul 02 09:11:14 UTC 2025
3 recovered 99.3 Wed Jul 02 10:24:19 UTC 2025
...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                      |
|------------------|---------------------------------------------------|
| 10.16.1000       | The <b>input-voltage</b> parameter is introduced. |
| 10.07 or earlier | --                                                |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show environment power-redundancy

show environment power-consumption [vsx-peer]

## Description

Displays power consumption information.

| Parameter  | Description                                                           |
|------------|-----------------------------------------------------------------------|
| [vsx-peer] | Optional. Display switch power redundancy information for a VSX peer. |

## Example

Showing the power redundancy is not configured

```
switch# # show env power-redundancy
Configured Operational
Redundancy Redundancy

n+n none
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.16   | Command introduced. |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

# show environment temperature

show environment temperature [detail] [vsx-peer]

## Description

Shows the temperature information from sensors in the switch that affect fan control.

| Parameter | Description                                              |
|-----------|----------------------------------------------------------|
| detail    | Shows detailed information from each temperature sensor. |

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Usage

Temperatures are shown in Celsius.

Valid values for status are the following: \

| Parameter    | Description                                                        |
|--------------|--------------------------------------------------------------------|
| normal       | Sensor is within nominal temperature range.                        |
| max          | Highest temperature from this sensor.                              |
| low_critical | Lowest threshold temperature for this sensor.                      |
| critical     | Highest threshold temperature for this sensor.                     |
| fault        | Fault event for this sensor.                                       |
| emergency    | Over temperature event for Over temperature event for this sensor. |

## Examples



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show events

```
show events [-e <EVENT-ID> |
 -s {emergency | alert | critical | error | warning | notice | info | debug} |
 -r |
 -a |
 -n <COUNT> |
```

```
-i <MEMBER-SLOT> |
-m {active | standby} |
-c {lldp | ospf | ...} |
-d {lldpd | bgpd | fand | ...}]
```

## Description

Shows event logs generated by the switch modules since the last reboot.

| Parameter                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-e &lt;EVENT-ID&gt;</code>                                                         | Shows the event logs for the specified event ID. Event ID range: 101 through 99999.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>-s {emergency   alert   critical   error   warning   notice   info   debug}</code> | Shows the event logs for the specified severity. Select the severity from the following list: <ul style="list-style-type: none"> <li>▪ <b>emergency</b>: Displays event logs with severity emergency only.</li> <li>▪ <b>alert</b>: Displays event logs with severity alert and above.</li> <li>▪ <b>critical</b>: Displays event logs with severity critical and above.</li> <li>▪ <b>error</b>: Displays event logs with severity error and above.</li> <li>▪ <b>warning</b>: Displays event logs with severity warning and above.</li> <li>▪ <b>notice</b>: Displays event logs with severity notice and above.</li> <li>▪ <b>info</b>: Displays event logs with severity info and above.</li> <li>▪ <b>debug</b>: Displays event logs with all severities.</li> </ul> |
| <code>-r</code>                                                                          | Shows the most recent event logs first.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <code>-a</code>                                                                          | Shows all event logs, including those events from previous boots.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <code>-n &lt;COUNT&gt;</code>                                                            | Displays the specified number of event logs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>-c {lldp   ospf   ...}</code>                                                      | Shows the event logs for the specified event category. Enter <b>show event -c</b> for a full listing of supported categories with descriptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>-d {lldpd   bgpd   fand   ...}</code>                                              | Shows the event logs for the specified process. Enter <b>show event -d</b> for a full listing of supported daemons with descriptions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Examples

Showing event logs:

```
switch# show events

show event logs

2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to
up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1
in Hardware
```

Showing the most recent event logs first:

```
switch# show events -r

show event logs

2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1
in Hardware
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to
up for bridge_normal interface
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
70:72:cf:51:50:7c
```

Showing all event logs:

```
switch# show events -a

show event logs

2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to
up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1
in Hardware
```

Showing event logs related to LACP:

```
switch# show events -c lacp

show event logs

2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
70:72:cf:51:50:7c
```

Showing event logs as per the specified member/slot ID:

```
switch# show events -i 1/1

show event logs

2017-08-17:22:32:25.743991|hpe-sysmond|6301|LOG_INFO|LC|1/1|System resource
utilization poll interval is changed to 313
2017-08-17:22:33:01.692860|hpe-sysmond|6301|LOG_INFO|LC|1/1|System resource
utilization poll interval is changed to 23
2017-08-17:22:33:06.181436|hpe-sysmond|6301|LOG_INFO|LC|1/1|System resource
utilization poll interval is changed to 512
2017-08-17:22:33:06.181436|systemd-coredump|1201|LOG_CRIT|LC|1/1|hpe-sysmond
crashed due to signal:11
```

Showing event logs as per the specified process:

```
switch# show events -d lacpd

show event logs

2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
70:72:cf:51:50:7c
```



Displaying the specified number of event logs:

```
switch# show events -n 5

show event logs

2018-03-21:06:12:15.500603|arpmgrd|6101|LOG_INFO|AMM|-|ARPMGRD daemon has started
2018-03-21:06:12:17.734405|lldpd|109|LOG_INFO|AMM|-|Configured LLDP tx-delay to 2
2018-03-21:06:12:17.740517|lacpd|1307|LOG_INFO|AMM|-|LACP system ID set to
70:72:cf:d4:34:42
2018-03-21:06:12:17.743491|vrfmgrd|5401|LOG_INFO|AMM|-|Created a vrf entity
42cc3df7-1113-412f-b5cb-e8227b8c22f2
2018-03-21:06:12:17.904008|vrfmgrd|5401|LOG_INFO|AMM|-|Created a vrf entity
4409133e-2071-4ab8-adfe-f9662c06b889
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                                  |
|---------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only. |

## show hostname

show hostname [vsx-peer]

### Description

Shows the current host name.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show images

show images [vsx-peer]

## Description

Shows information about the software in the primary and secondary images.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

Showing the primary and secondary images on a 8320 switch:

```
switch# show images

AOS-CX Primary Image

Version : TL.10.05.0001I
Size : 405 MB
Date : 2020-04-23 02:49:04 PDT
SHA-256 : 7efe86a445e87e40f47de156add25720b7277cae1a8db2f9c4ea5f49e74f2a5a

AOS-CX Secondary Image
```

```

Version : TL.10.05.0001I
Size : 405 MB
Date : 2020-04-23 02:49:04 PDT
SHA-256 : 7efe86a445e87e40f47de156add25720b7277cae1a8db2f9c4ea5f49e74f2a5a

Default Image : primary

Management Module 1/1 (Active)

Active Image : primary
Service OS Version : TL.01.05.0002-internal
BIOS Version : TL-01-0013

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ip errors

```
show ip errors [{vrf <vrf-name>}|all-vrfs]
```

### Description

Shows hardware and software IP error statistics for packets received by the switch since the switch was last booted. If none of the optional VRF parameters are included, the **show ip errors** command displays the current system-wide hardware IP error counters and the default VRF's software IP error counters on the switch.

| Parameter      | Description                                                                   |
|----------------|-------------------------------------------------------------------------------|
| vrf <vrf-name> | Optional. Display hardware and software IP error counters for a specific VRF. |
| all-vrfs       | Optional. Display hardware and software IP error counters for all VRFs.       |

### Usage

IP error info about received packets is collected from each active line card on the switch and is preserved during failover events. Error counts are cleared when the switch is rebooted.

Drop reasons may include the following:

#### ■ Malformed packet

The packet does not conform to TCP/IP protocol standards such as packet length or internet header length.

A large number of malformed packets can indicate that there are hardware malfunctions such as loose cables, network card malfunctions, or that a DOS (denial of service) attack is occurring.

#### ■ IP address error

The packet has an error in the destination or source IP address. Examples of IP address errors include the following:

- The source IP address and destination IP address are the same.
- There is no destination IP address.
- The source IP address is a multicast IP address.
- The forwarding header of an IPv6 address is empty.
- There is no source IP address for an IPv6 packet.

#### ■ Invalid TTLs

The TTL (time to live) value of the packet reached zero. The packet was discarded because it traversed the maximum number of hops permitted by the TTL value.

TTLs are used to prevent packets from being circulated on the network endlessly.

### Example

Showing the current system-wide hardware IP error counters and the default VRF's software IP error counters on the switch:

```
switch# show ip errors
System-wide (hardware) IP errors

Drop reason Packets

Malformed packets 1
IP address errors 10
Per-VRF (software) IP errors

VRF
Drop reason Packets

default
IPv4 maximum transmission unit 3
IPv4 time to live 0
IPv6 maximum transmission unit 0
IPv6 hop limit 6

Malformed packets 1
...

```

Showing the current system-wide hardware IP error counter and the software IP error counter for all VRFs on the switch.

```

switch# show ip errors all-vrfs
System-wide (hardware) IP errors

Drop reason Packets

Malformed packets 1
IP address errors 10
Per-VRF (software) IP errors

VRF
Drop reason Packets

default
IPv4 maximum transmission unit 3
IPv4 time to live 0
IPv6 maximum transmission unit 0
IPv6 hop limit 6
red
IPv4 maximum transmission unit 3
IPv4 time to live 7
IPv6 maximum transmission unit 0
IPv6 hop limit 6
blue
IPv4 maximum transmission unit 0
IPv4 time to live 1
IPv6 maximum transmission unit 0
IPv6 hop limit 6
...

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                                           |
|------------------|----------------------------------------------------------------------------------------|
| 10.14.1000       | Command updated to display both hardware and software IP errors in the command output. |
| 10.07 or earlier | --                                                                                     |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show module

show module [vsx-peer]

## Description

Shows information about installed line modules and management modules.



Although this switch does not have removable modules, this command will still return information about the switch, referring to management modules and line modules.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vsx-peer</code> | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Usage

Identifies and shows status information about the line modules and management modules that are installed in the switch.

To show the configuration information—if any—associated with that line module slot, use the **show running-configuration** command.

Status is one of the following values:

**Active**

This switch is the active management module.

**Standby**

This switch is the standby management module.

**Deinitializing**

The switch is being deinitialized.

**Diagnostic**

The switch is in a state used for troubleshooting.

**Down**

The switch is physically present but is powered down.

**Empty**

The switch hardware is not installed in the chassis.

**Failed**

The switch has experienced an error and failed.

**Failover**

This switch is a fabric module or a line module, and it is in the process of connecting to the new active management module during a management module failover event.

**Initializing**

The switch is being initialized.

**Present**

The switch hardware is installed in the chassis.

**Ready**

The switch is available for use.

**Updating**

A firmware update is being applied to the switch.

## Examples

Showing all installed modules on an 8320 switch:



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show running-config

show running-config [<FEATURE>] [all] [vsx-peer]

### Description

Shows the current nondefault configuration running on the switch. No user information is displayed.

| Parameter       | Description                                                                                                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <FEATURE>       | Specifies the name of a feature. For a list of feature names, enter the <code>show running-config</code> command, followed by a space, followed by a question mark (?). When the <code>json</code> parameter is used, the <code>vsx-peer</code> parameter is not applicable. |
| <i>all</i>      | Shows all default values for the current running configuration.                                                                                                                                                                                                              |
| <i>vsx-peer</i> | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                             |

### Examples

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version AOS-CX 10.0X.XXXX
!
lldp enable
linecard-module LC1 part-number JL363A
vrf green
!
!
!
!
!
!
aaa authentication login default local
aaa authorization commands default none
!
!
```

```

!
!
vlan 1
 no shutdown
vlan 20
 no shutdown
vlan 30
 no shutdown
interface 1/1/1
 no shutdown
 no routing
 vlan access 30
interface 1/1/32
 no shutdown
 no routing
 vlan access 20
interface bridge_normal-1
 no shutdown
interface bridge_normal-2
 no shutdown
interface vlan20
 no shutdown
 vrf attach green
 ip address 20.0.0.44/24
 ip ospf 1 area 0.0.0.0
 ip pim-sparse enable

interface vlan30
 no shutdown
 vrf attach green
 ip address 30.0.0.44/24
 ip ospf 1 area 0.0.0.0
 ip pim-sparse enable

 ip pim-sparse hello-interval 100

```

Showing the current running configuration in json format:

```

switch> show running-config json
Running-configuration in JSON:
{
 "Monitoring_Policy_Script": {
 "system_resource_monitor_mm1.1.0": {
 "Monitoring_Policy_Instance": {
 "system_resource_monitor_mm1.1.0/system_resource_monitor_
mm1.1.0.default": {
 "name": "system_resource_monitor_mm1.1.0.default",
 "origin": "system",
 "parameters_values": {
 "long_term_high_threshold": "70",
 "long_term_normal_threshold": "60",
 "long_term_time_period": "480",
 "medium_term_high_threshold": "80",
 "medium_term_normal_threshold": "60",
 "medium_term_time_period": "120",
 "short_term_high_threshold": "90",
 "short_term_normal_threshold": "80",
 "short_term_time_period": "5"
 }
 }
 }
 }
 },

```



```
...
...
...
...
```

Show the current running configuration without default values:

```
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
!
!
!
vlan 1
switch(config)# show running-config all
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
!
!
!
vlan 1
switch(config)#
```

Show the current running configuration with default values:

```
switch(config)# snmp-server vrf mgmt
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
snmp-server vrf mgmt
!
!
!
!
!
vlan 1
switch(config)#
```

```

switch(config)#
switch(config)# show running-config all
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
snmp-server vrf mgmt
snmp-server agent-port 161
snmp-server community public
!
!
!
!
vlan 1
switch(config)#

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show running-config current-context

show running-config current-context

## Description

Shows the current non-default configuration running on the switch in the current command context.

## Usage

You can enter this command from the following configuration contexts:

- Any child of the global configuration (**config**) context. If the child context has instances—such as interfaces—you can enter the command in the context of a specific instance. Support for this command is provided for one level below the **config** context. For example, entering this command for a child of a child of the `config` context not supported. If you enter the command on a child of the **config** context, the current configuration of that context and the children of that context are

displayed.

- The global configuration (**config**) context. If you enter this command in the global configuration (**config**) context, it shows the running configuration of the entire switch. Use the **show running-configuration** command instead.

## Examples

Showing the running configuration for the current interface:

```
switch(config-if)# show running-config current-context
interface 1/1/1
vsx-sync qos vlans
 no shutdown
 description Example interface
 no routing
vlan access 1
exit
```

Showing the current running configuration for the management interface:

```
switch(config-if-mgmt)# show running-config current-context
interface mgmt
 no shutdown
 ip static 10.0.0.1/24
 default-gateway 10.0.0.8
 nameserver 10.0.0.1
```

Showing the running configuration for the external storage share named **nasfiles**:

```
switch(config-external-storage-nasfiles)# show running-config current-context
external-storage nasfiles
 address 192.168.0.1
 vrf default
 username nasuser
 password ciphertext
 AQBapalKj+XMsZumHEwIc9OR6YcOw5Z6Bh9rV+9ZtKDKzvbaBAAAAB1CTrM=
 type scp
 directory /home/nas
 enable
switch(config-external-storage-nasfiles)#
```

Showing the running configuration for a context that does not have instances:

```
switch(config-vsx)# show run current-context
vsx
 inter-switch-link 1/1/1
 role secondary
 vsx-sync sflow time
```



---

For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                    | Authority                                                                          |
|---------------|--------------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code> or a child of <code>config</code> . See Usage. | Administrators or local user group members with execution rights for this command. |

## show startup-config

`show startup-config [json]`

### Description

Shows the contents of the startup configuration.



Switches in the `factory-default` configuration do not have a startup configuration to display.

| Parameter         | Description                    |
|-------------------|--------------------------------|
| <code>json</code> | Display output in JSON format. |

### Examples

Showing the startup-configuration in non-JSON format for an 8320 switch:

Showing the startup-configuration in JSON format:

```
switch# show startup-config json
Startup configuration:
{
 "AAA_Server_Group": {
 "local": {
 "group_name": "local"
 },
 "none": {
 "group_name": "none"
 }
 },
 ...
}
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show system

```
show system [serviceos password-prompt] [vsx-peer]
```

### Description

Shows general status information about the system.

| Parameter                              | Description                                                                                                                                                                                                                      |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>serviceos password-prompt</code> | Shows the Service OS password prompt status.                                                                                                                                                                                     |
| <code>vsx-peer</code>                  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Usage

CPU utilization represents the average utilization across all the CPU cores.

System Description, System Contact, and System Location can be set with the `snmp-server` command.

When `vsx-peer` is specified, the `Up Time` value is not shown because it is not synchronized between VSX peers.

### Examples

Showing system information:

```
switch# show system
Hostname : switch
System Description : switch description
System Contact : contact
System Location : location

Vendor : Aruba
Product Name : XXXXXX ...
Chassis Serial Nbr : XXXXXXXXXXXX
Base MAC Address : xxxxxx-xxxxxx
AOS-CX Version : XX.99.99.9999

Time Zone : UTC

Up Time : 1 week, 5 hours, 28 minutes
CPU Util (%) : 5
CPU Util (% avg 1 min) : 11
CPU Util (% avg 5 min) : 10
Memory Usage (%) : 35
```

Showing the Service OS password prompt status:

```
switch# show system serviceos password-prompt
password-prompt: disabled
```

Showing system information for a VSX primary and secondary (peer) switch:

```
switch# show system
Hostname : vsx-primary
System Description : switch description
System Contact : contact
System Location : location

Vendor : Aruba
Product Name : XXXXXX ...
Chassis Serial Nbr : XXXXXXXXXXXX
Base MAC Address : xxxxxx-xxxxxx

Hostname : vsx-primary
System Description : switch description
System Contact : contact
System Location : location

Vendor : Aruba
Product Name : XXXXXX ...
Chassis Serial Nbr : XXXXXXXXXXXX
Base MAC Address : xxxxxx-xxxxxx
AOS-CX Version : XX.99.99.9999

Time Zone : UTC

Up Time : 1 week, 2 hours, 15 minutes
CPU Util (%) : 15
CPU Util (% avg 1 min) : 12
CPU Util (% avg 5 min) : 8
Memory Usage (%) : 37

switch# show system vsx-peer
Hostname : vsx-secondary
System Description : switch description
System Contact : contact
System Location : location

Vendor : Aruba
Product Name : XXXXXX ...
Chassis Serial Nbr : XXXXXXXXXXXX
Base MAC Address : xxxxxx-xxxxxx
AOS-CX Version : XX.99.99.9999

Time Zone : UTC

CPU Util (%) : 7
CPU Util (% avg 1 min) : 13
CPU Util (% avg 5 min) : 9
Memory Usage (%) : 32
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                             |
|------------------|----------------------------------------------------------|
| 10.12            | Added CPU Util (% avg 1 min) and CPU Util (% avg 5 min). |
| 10.07 or earlier | --                                                       |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show system resource-utilization

show system resource-utilization [all | daemon <DAEMON-NAME>] [vsx-peer]

### Description

Shows the system resource utilization data.

| Parameter            | Description                                                                                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all                  | Shows the resource utilization data for the entire switch.                                                                                                                                                                       |
| daemon <DAEMON-NAME> | Shows only the resource utilization data for the process identified by <DAEMON-NAME>.                                                                                                                                            |
| vsx-peer             | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Usage

For a list of daemons that log events, enter `show events -d ?` from a switch prompt in the manager (#) context.

### Examples

Showing system resource utilization data:

```
switch# show system resource-utilization
System Resources:
Processes : 144
CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 22
Open FD's : 1358
Storage 1: Endurance utilization = 10-20% (mmc-type-a), 0-10% (mmc-type-b),
Health = normal
```

```
Data written to various partitions since boot
Nos : 5 MB
Log : 1 MB
Coredump : 23 MB
Security : 2 MB
Selftest : 405 KB
Swap : 14 MB
```

```
Storage partition usage(%)
Nos : 5
Log : 60
Coredump : 23
Security : 2
Selftest : 1
Swap : 0
```

| Process     | CPU Usage(%) | Memory Usage(%) | Open FD's |
|-------------|--------------|-----------------|-----------|
| hpe-sysmond | 1            | 2               | 11        |
| hpe-mgmdd   | 0            | 1               | 5         |
| ...         |              |                 |           |

Attempting to show resource utilization data when system resource utilization polling is disabled:

```
switch# show system resource-utilization
System resource utilization data poll is currently disabled
```

Showing the resource utilization data for a particular process:

```
switch# show system resource-utilization daemon hpe-sysmond
Process CPU Usage(%) Memory Usage(%) Open FD's

hpe-sysmond 1 2 11
```

Showing system resource utilization data for all:

```
switch# show system resource-utilization all

Resource utilization data for Management Module

System Resources:
Processes : 244
CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 1854
Storage 1: Endurance utilization = 0-10% (mmc-type-a), 0-10% (mmc-type-b),
Health = normal

Data written to various partitions since boot
Nos : 15 MB
Log : 1 MB
```



```
Coredump : 23 MB
Security : 2 MB
Selftest : 405 KB
Swap : 0 KB
```

Storage partition usage(%)

```
Nos : 5
Log : 60
Coredump : 23
Security : 2
Selftest : 1
Swap : 0
```

| Process       | CPU Usage(%) | Memory Usage(%) | Open FD's |
|---------------|--------------|-----------------|-----------|
| (sd-pam)      | 0            | 0               | 7         |
| aautilspamcfg | 0            | 1               | 10        |
| ...           |              |                 |           |

Showing CPU/RAM field for a specific line module:

```
switch# show system resource-utilization module 1/5
```

```

System Resource utilization for line card module: 1/5

```

```
CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 754
Memory usage in kilobytes:
Physical Memory : 3066796 KB
Reserved Memory : 244804 KB
Used Memory : 1216800 KB
Free Memory : 1849996 KB
```

Showing CPU/RAM field for the standby management module:

```
switch# show system resource-utilization standby
```

```
System Resources:
```

```
Processes : 244
CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 1854
Storage 1: Endurance utilization = 10-20% (mmc-type-a), 0-10% (mmc-type-b), Health
= normal
Data written to various partitions since boot
Nos : 15 MB
Log : 1 MB
Coredump : 23 MB
Security : 2 MB
Selftest : 405 KB
Swap : 14 MB
Storage partition usage(%)
Nos : 5
Log : 60
```

```

Coredump : 23
Security : 2
Selftest : 1
Swap : 0
Memory usage in kilobytes:
Physical Memory : 7274948 KB
Reserved Memory : 1580224 KB
Used Memory : 1614416 KB
Free Memory : 5660532 KB

```

Showing CPU/RAM field for a specific member ID:

```

switch# show system resource-utilization all

Resource utilization data for vsf member 1

System Resources:
Processes : 244
CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 1854
Storage 1: Endurance utilization = 0-10% (mmc-type-a), 0-10% (mmc-type-b), Health
= normal
Data written to various partitions since boot
Nos : 15 MB
Log : 1 MB
Coredump : 23 MB
Security : 2 MB
Selftest : 405 KB
Swap : 14 MB
Storage partition usage(%)
Nos : 5
Log : 60
Coredump : 23
Security : 2
Selftest : 1
Swap : 0
Memory usage in kilobytes:
Physical Memory : 7274948 KB
Reserved Memory : 1580224 KB
Used Memory : 1614416 KB
Free Memory : 5660532 KB

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                                                   |
|---------|----------------------------------------------------------------|
| 10.17   | Added CPU/RAM field                                            |
| 10.12   | The output of this command includes <b>CPU usage(% average</b> |

| Release          | Modification                                                          |
|------------------|-----------------------------------------------------------------------|
|                  | <b>over 1 minute)</b> and <b>CPU usage(% average over 5 minute)</b> . |
| 10.07 or earlier | --                                                                    |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show tech

```
show tech [basic | <FEATURE>] [local-file]
```

### Description

Shows detailed information about switch features by automatically running the `show` commands associated with the feature. If no parameters are specified, the `show tech` command shows information about all switch features. Technical support personnel use the output from this command for troubleshooting.

| Parameter                    | Description                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>basic</code>           | Specifies showing a basic set of information.                                                                                                                 |
| <code>&lt;FEATURE&gt;</code> | Specifies the name of a feature. For a list of feature names, enter the <code>show tech</code> command, followed by a space, followed by a question mark (?). |
| <code>local-file</code>      | Shows the output of the <code>show tech</code> command to a local text file.                                                                                  |

### Usage

To terminate the output of the `show tech` command, enter **Ctrl+C**.

If the command was not terminated with **Ctrl+C**, at the end of the output, the `show tech` command shows the following:

- The time consumed to execute the command.
- The list of failed `show` commands, if any.

To get a copy of the local text file content created with the `show tech` command that is used with the `local-file` parameter, use the `copy show-tech local-file` command.

### Example

Showing the basic set of system information:

```
switch# show tech basic
=====
Show Tech executed on Wed Sep 6 16:50:37 2017
```

```

=====
=====
[Begin] Feature basic
=====

Command : show core-dump all

no core dumps are present

...

[End] Feature basic
=====

=====
1 show tech command failed
=====
Failed command:
 1. show boot-history
=====
Show tech took 3.000000 seconds for execution

```

Directing the output of the **show tech basic** command to the local text file:

```

switch# show tech basic local-file
Show Tech output stored in local-file. Please use 'copy show-tech local-file'
to copy-out this file.

```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show usb

show usb [vsx-peer]

### Description

Shows the USB port configuration and mount settings.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

If USB has not been enabled:

```
switch> show usb
Enabled: No
Mounted: No
```

If USB has been enabled, but no device has been mounted:

```
switch> show usb
Enabled: Yes
Mounted: No
```

If USB has been enabled and a device mounted:

```
switch> show usb
Enabled: Yes
Mounted: Yes
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show usb file-system

```
show usb file-system [<PATH>]
```

## Description

Shows directory listings for a mounted USB device. When entered without the <PATH> parameter the top level directory tree is shown.

| Parameter | Description                                                             |
|-----------|-------------------------------------------------------------------------|
| <PATH>    | Specifies the file path to show. A leading "/" in the path is optional. |

## Usage

Adding a leading "/" as the first character of the <PATH> parameter is optional.

Attempting to enter '..' as any part of the <PATH> will generate an invalid path argument error. Only fully-qualified path names are supported.

## Examples

Showing the top level directory tree:

```
switch# show usb file-system
/mnt/usb:
'System Volume Information' dir1'

/mnt/usb/System Volume Information':
IndexerVolumeGuid WPSettings.dat

/mnt/usb/dir1:
dir2 test1

/mnt/usb/dir1/dir2:
test2
```

Showing available path options from the top level:

```
switch# show usb file-system /
total 64
drwxrwxrwx 2 32768 Jan 22 16:27 'System Volume Information'
drwxrwxrwx 3 32768 Mar 5 15:26 dir1
```

Showing the contents of a specific folder:

```
switch# show usb file-system /dir1
total 32
drwxrwxrwx 2 32768 Mar 5 15:26 dir2
-rwxrwxrwx 1 0 Feb 5 18:08 test1

switch# show usb file-system dir1/dir2
total 0
-rwxrwxrwx 1 0 Feb 6 05:35 test2
```

Attempting to enter an invalid character in the path:

```
switch# show usb file-system dir1/../../
Invalid path argument
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show version

`show version [vsx-peer]`

### Description

Shows version information about the network operating system software, service operating system software, and BIOS.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vsx-peer</code> | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# system resource-utilization poll-interval

system resource-utilization poll-interval <SECONDS>

## Description

Configures the polling interval for system resource information collection and recording such as CPU and memory usage.

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| <SECONDS> | Specifies the poll interval in seconds. Range: 10-3600. Default: 10. |

## Example

Configuring the system resource utilization poll interval:

```
switch(config)# system resource-utilization poll-interval 20
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## top cpu

top cpu

## Description

Shows CPU utilization information.

## Example

Showing top CPU information:

```
switch# top cpu
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks: 76 total, 2 running, 74 sleeping, 0 stopped, 0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total, 2487508 free, 897040 used, 661948 buff/cache
```



```
KiB Swap: 0 total, 0 free, 0 used, 2859196 avail Mem

 PID USER PRI NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 ...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# top memory

top memory

## Description

Shows memory utilization information.

## Example

Showing top memory:

```
switch> top memory
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks: 76 total, 2 running, 74 sleeping, 0 stopped, 0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total, 2487508 free, 897040 used, 661948 buff/cache
KiB Swap: 0 total, 0 free, 0 used, 2859196 avail Mem

 PID USER PRI NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
 ...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## usb

usb  
no usb

## Description

Enables the USB ports on the switch. This setting is persistent across switch reboots and management module failovers. Both active and standby management modules are affected by this setting.

The **no** form of this command disables the USB ports.

## Example

Enabling USB ports:

```
switch(config)# usb
```

Disabling USB ports when a USB drive is mounted:

```
switch(config)# no usb
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# usb mount | unmount

usb {mount | unmount}

## Description

Enables or disables the inserted USB drive.

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| mount     | Enables the inserted USB drive.                             |
| unmount   | Disables the inserted USB drive in preparation for removal. |

## Usage

If USB has been enabled in the configuration, the USB port on the active management module is available for mounting a USB drive. The USB port on the standby management module is not available.

An inserted USB drive must be mounted each time the switch boots or fails over to a different management module.

A USB drive must be unmounted before removal.

The supported USB file systems are FAT16 and FAT32.

## Examples

Mounting a USB drive in the USB port:

```
switch# usb mount
```

Unmounting a USB drive:

```
switch# usb unmount
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### profile

```
profile <PROFILE-NAME>
no profile [<PROFILE-NAME>]
```

#### Description

Selects the system profile. System profiles set the overall capabilities and capacities of the switch based on the selected profile used at boot time. Switch profiles set capacities such as that of the hardware forwarding table. Use command [show profiles available](#) to show the details of each available profile.



When a switch is configured with a non-default profile, the switch requires a reboot for the profile to be applied. You are prompted for the reboot.

The **no** form of this command resets the specified profile to its defaults.

#### Usage

Profiles supported on 8320, 8325/8325H/8325P and 10000 Switch Series:

| Profile names | Description                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L3-agg        | Optimizes for layer 3 forwarding with more table space allocated to host(ARP/ND) entries.                                                                         |
| L3-core       | (The default on the 8320 Switch Series.) Optimize for layer 3 forwarding with more table space allocated to route entries.                                        |
| Leaf          | (The default on the 8325/8325H/8325P, and 10000 Switch Series.) Optimizes for layer 2 forwarding with more table space allocated to overlay host entries (VXLAN). |
| spine         | Optimizes for layer 3 forwarding with more table space allocated to route entries.                                                                                |

Profiles supported on 9300 and 9300S Switch series:

| Profile names      | Description                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------|
| Leaf               | Optimizes for layer 2 forwarding with more table space allocated to overlay host entries (VXLAN). |
| spine              | Optimizes for layer 3 forwarding with more table space allocated to route entries.                |
| DC-Optimized-Spine | Spine profile optimized for datacenter deployments. The DC-                                       |

| Profile names     | Description                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | Optimized-Spine profile does not support IP tunnels, including 6in4 tunnels, 6in6 tunnels, and GRE tunnels.                                                                                                             |
| DC-Optimized-Leaf | (The default on the 9300/9300S Switch Series.) Leaf profile optimized for datacenter deployments. The DC-Optimized-leaf profile does not support IP tunnels, including 6-in-4 tunnels, 6-in-6 tunnels, and GRE tunnels. |

## Examples

(8320, 8325, 9300, 10000) Selecting the L3-agg profile and then rebooting the system:

```
switch(config)# profile l3-agg
switch(config)# exit
switch# boot system
...
```

(8320, 8325, 9300, 10000) Selecting the Spine profile and then rebooting the system:

```
switch(config)# profile Spine
switch(config)# exit
switch# boot system
...
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## show profiles available

```
show profiles available
```

### Description

Shows all system profile names available and profile details.

### Examples

Showing all available profiles for a 9300 switch:

```
switch# show profiles available
```

#### Available Profiles

```

DC-Optimized-Leaf MAC Addresses 81920, Unicast Routes(IPv4: 65536, IPv6:
32768), Host-Routes/Hosts(IPv4: 163840, IPv6: 81920), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765)
(Default)
```

```
DC-Optimized-Spine MAC Addresses 32768, Unicast Routes(IPv4: 1269760, IPv6:
624640), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742)
```

```
Leaf MAC Addresses 81920, Unicast Routes(IPv4: 65536, IPv6:
32768), Host-Routes/Hosts(IPv4: 163840, IPv6: 81920), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765), Legacy Profile
```

```
Spine MAC Addresses 32768, Unicast Routes(IPv4: 1269760, IPv6:
624640), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742), Legacy Profile
```

Showing all available profiles for a 9300S switch:

```
switch# show profiles available
```

#### Available Profiles

```

DC-Optimized-Leaf MAC Addresses 49152, Unicast Routes(IPv4: 32269, IPv6:
16885), Host-Routes/Hosts(IPv4: 98304, IPv6: 49152), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765) (Default)
```

```
DC-Optimized-Spine MAC Addresses 32768, Unicast Routes(IPv4: 720527, IPv6:
368404), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742)
```

```
Leaf MAC Addresses 49152, Unicast Routes(IPv4: 32269, IPv6:
16885), Host-Routes/Hosts(IPv4: 98304, IPv6: 49152), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765), Legacy Profile
```

```
Spine MAC Addresses 32768, Unicast Routes(IPv4: 720527, IPv6:
368404), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742), Legacy Profile
```



---

Starting with AOS-CX 10.16.1005, DC-Optimized-Leaf is the default profile for the 9300 and 9300S Switch Series. DC-Optimized-Leaf and DC-Optimized-Spine profiles do not support IP tunnels, including 6in4 tunnels, 6in6 tunnels, and GRE tunnels.

---



---

For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

---

## Command History

| Release          | Modification                                                                                 |
|------------------|----------------------------------------------------------------------------------------------|
| 10.16.1005       | DC-Optimized-Leaf and DC-Optimized-Leaf profiles introduced on 9300 and 9300S Switch series. |
| 10.07 or earlier | --                                                                                           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show profile current

show profile current

## Description

Shows the current system profile.

## Examples

Showing the current profile on the 9300 and 9300S:

```
switch# show profile current
Current profile

DC-Optimized-Leaf
```

```
switch# show profile current

Current profile

L3-core
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |



## show telnet server

show telnet server

### Description

Shows the Telnet server configuration.

### Examples

Showing the Telnet server configuration:

```
switch(config)# show telnet server
TELNET Server Configuration:

 IP Version : IPv4
 TCP Port : 23
 Enabled VRFs : default, vrf1, vrf2,
 red, green
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

### Command History

| Release | Modification                               |
|---------|--------------------------------------------|
| 10.11   | Command introduced on all other platforms. |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## show telnet server sessions

show telnet server sessions [vrf <VRF-NAME> | all-vrfs]

### Description

Shows all active Telnet sessions for the specified VRF or all VRFs. If no VRF is provided, the Telnet sessions on the **default** VRF are shown.



The **mgmt** VRF and custom VRFs are not supported on 4100i, 6000, and 6100 switches.

| Parameter                         | Description                                       |
|-----------------------------------|---------------------------------------------------|
| <code>vrf &lt;VRF-NAME&gt;</code> | Specifies the Telnet sessions for a specific VRF. |
| <code>all-vrfs</code>             | Specifies the Telnet sessions for all VRFs        |

## Examples

Showing the Telnet session on the **default** VRF:

```
switch(config)# show telnet server sessions
TELNET sessions on VRF default:

IPv4 TELNET Sessions:
 Server IP : 10.1.1.1
 Client IP : 10.1.1.2
 Client Port : 58835
```

The following example shows the Telnet sessions on all VRFs. If only the **default** VRF is supported by the switch, only the **default** VRF will display in the output of this command.

```
switch(config)# show telnet server sessions all-vrfs
TELNET sessions on VRF mgmt:

IPv4 TELNET Sessions:
 Server IP : 10.1.1.1
 Client IP : 10.1.1.2
 Client Port : 58835

TELNET sessions on VRF default:

IPv4 TELNET Sessions:
 Server IP : 20.1.1.1
 Client IP : 20.1.1.2
 Client Port : 58837
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                               |
|---------|--------------------------------------------|
| 10.11   | Command introduced on all other platforms. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## telnet server

```
telnet server vrf <VRF-NAME>
no telnet server vrf <VRF-NAME>
```

### Description

Enables the Telnet server on the desired VRF. Telnet server is disabled by default. The **no** form of this command disables the Telnet server.



The **mgmt** VRF and custom VRFs are not supported on 4100i, 6000, and 6100 switches.

| Parameter      | Description                                                               |
|----------------|---------------------------------------------------------------------------|
| vrf <VRF-NAME> | Specifies the VRF on which the Telnet server will be enabled or disabled. |

### Examples

Configuring the Telnet server on the **default** VRF:

```
switch(config)# telnet server vrf default
```

Configuring the Telnet server on the **mgmt** VRF:

```
switch(config)# telnet server vrf mgmt
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release | Modification                                                |
|---------|-------------------------------------------------------------|
| 10.11   | Command introduced on 9300, 1000, 4100i and 8xxx platforms. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## logging console {notify | severity | filter}

```
logging console{notify <event|debug|all> | severity <level> | filter keyword}
```

```
no logging console
```

### Description

Enables the logging console feature in the console session. It display all debug log or event log or both debug and event log messages. Monitoring can be filtered with the severity options or with the help of keywords. Enabling terminal monitor without options displays both debug and event log with a severity error. This command is persistent across reboot.

The **no** form of this command disables the terminal monitor configuration.

| Parameter                                   | Description                                                                                                                                                                                                                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>notify &lt;event debug all&gt;</code> | Specifies the type of log notification. <ul style="list-style-type: none"><li>▪ <b>Event:</b> Displays the event log messages. (Default)</li><li>▪ <b>Debug:</b> Displays the debug log messages.</li><li>▪ <b>All:</b> Displays both event and debug log messages.</li></ul> |
| <code>severity &lt;level&gt;</code>         | Specifies the severity level for the logs. The different severity levels are emergency, critical, error, warning, notice, information (default), alert, and debug (shows all severities).                                                                                     |
| <code>filter &lt;keyword&gt;</code>         | Specifies the filter by applying keyword for the logs.                                                                                                                                                                                                                        |

### Authority

Administrators or local user group members with execution rights for this command.

### Examples

Configuring console logging in the console session:

```
switch(config)# logging console
Terminal-monitor is enabled successfully

switch(config)# logging console notify all
Terminal-monitor is enabled successfully

switch(config)# logging console notify event severity info
Terminal-monitor is enabled successfully

switch(config)# logging console filter lldp
Terminal-monitor is enabled successfully
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.08   | Feature introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# show terminal-monitor

show terminal-monitor

## Description

Shows whether the terminal monitoring is enabled or disabled.



This command will not show any information about console logging.

## Examples

Displaying terminal monitor when enabled:

```
switch# show terminal-monitor

Terminal-monitor is enabled

Notify | Severity | Filter

event debug lldp

```

Displaying terminal monitor when disabled:

```
switch# show terminal-monitor

Terminal-monitor is disabled
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## terminal-monitor {notify | severity | filter}

```
terminal-monitor {notify <event|debug|all> | severity <level> | filter <keyword>}
```

```
no terminal-monitor
```

### Description

Enables and saves the terminal monitor feature in the switch configuration. It displays all debug log or event log or both debug and event log messages. Terminal monitoring can be filtered with the severity options or with the help of keywords. Enabling terminal monitor without options displays both debug and event log with a severity error.

The **no** form of this command removes the terminal monitor feature from the switch configuration and the command will not persist.

| Parameter                                   | Description                                                                                                                                                                                                                                                                       |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>notify &lt;event debug all&gt;</code> | Specifies the type of log notification. <ul style="list-style-type: none"> <li>▪ <b>Event:</b> Displays the event log messages. (Default)</li> <li>▪ <b>Debug:</b> Displays the debug log messages.</li> <li>▪ <b>All:</b> Displays both event and debug log messages.</li> </ul> |
| <code>severity &lt;level&gt;</code>         | Specifies the severity level for the logs. The different severity levels are emergency, critical, error, warning, notice, information (default), alert, and debug (shows all severities).                                                                                         |
| <code>filter &lt;keyword&gt;</code>         | Specifies the filter by applying keyword for the logs.                                                                                                                                                                                                                            |

### Authority

Administrators or local user group members with execution rights for this command.

### Examples

Enabling terminal monitor:

```
switch# terminal-monitor
Terminal-monitor is enabled successfully

switch# terminal-monitor notify all
Terminal-monitor is enabled successfully

switch# terminal-monitor notify event severity info
```

```
Terminal-monitor is enabled successfully

switch# terminal-monitor filter lldp
Terminal-monitor is enabled successfully
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### traceroute

```
traceroute {<IPV4-ADDR> | <HOSTNAME>} [ip-option loosesourceroute <IPV4-ADDR>] [dstport <NUMBER> | maxttl <NUMBER> | minttl <NUMBER> | probes <NUMBER> | timeout <TIME>] [vrf <VRF-NAME>] source {<IPV4-ADDR> | <IFNAME>}
```



Traceroute over VXLAN with `ip-option loosesourceroute` on L3VNI is not supported.

### Description

Uses traceroute for the specified IPv4 address or hostname with or without optional parameters.

| Parameter                       | Description                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| IPv4-address <IPV4-ADDR>        | Specifies the IPv4 address.                                                                                                                      |
| hostname                        | Specifies the hostname of the device to traceroute.                                                                                              |
| ip-option                       | Specifies the IP option.                                                                                                                         |
| loosesourceroute <IPV4-ADDR>    | Specifies the route for loose source record route. Enter one or more intermediate router IP addresses separated by ',' for loose source routing. |
| dstport <NUMBER>                | Specifies the destination port, <1-34000>. Default: 33434                                                                                        |
| maxttl <NUMBER>                 | Specifies the maximum number of hops to reach the destination, <1-255>. Default: 30                                                              |
| minttl <NUMBER>                 | Specifies the Minimum number of hops to reach the destination, <1-255>. Default: 1                                                               |
| probes <NUMBER>                 | Specifies the number of probes, <1-5>. Default: 3                                                                                                |
| timeout <TIME>                  | Specifies the traceroute timeout in seconds, <1-60>. Default: 3 seconds                                                                          |
| vrf <VRF-NAME>                  | Specifies the virtual routing and forwarding (VRF) to use .                                                                                      |
| source {<IPV4-ADDR>   <IFNAME>} | Specifies the source IPv4 address or interface name.                                                                                             |

### Usage

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.



## Examples

```
switch# traceroute 10.0.10.1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
 1 10.0.40.2 0.002ms 0.002ms 0.001ms
 2 10.0.30.1 0.002ms 0.001ms 0.001ms
 3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute localhost
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
 1 127.0.0.1 0.018ms 0.006ms 0.003ms

switch# traceroute 10.0.10.1 maxttl 20
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 3 sec. timeout, 3
probes
 1 10.0.40.2 0.002ms 0.002ms 0.001ms
 2 10.0.30.1 0.002ms 0.001ms 0.001ms
 3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute 10.0.10.1 minttl 1
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
 1 10.0.40.2 0.002ms 0.002ms 0.001ms
 2 10.0.30.1 0.002ms 0.001ms 0.001ms
 3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute 10.0.10.1 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
 1 10.0.40.2 0.002ms 0.002ms 0.001ms
 2 10.0.30.1 0.002ms 0.001ms 0.001ms
 3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute 10.0.10.1 probes 2
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 2
probes
 1 10.0.40.2 0.002ms 0.002ms
 2 10.0.30.1 0.002ms 0.001ms
 3 10.0.10.1 0.001ms 0.002ms

switch# traceroute 10.0.10.1 timeout 5
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 5 sec. timeout, 3
probes
 1 10.0.40.2 0.002ms 0.002ms 0.001ms
 2 10.0.30.1 0.002ms 0.001ms 0.001ms
 3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute localhost vrf red
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
 1 127.0.0.1 0.003ms 0.002ms 0.001ms

switch# traceroute localhost mgmt
traceroute to localhost (127.0.0.1), 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
 1 127.0.0.1 0.018ms 0.006ms 0.003ms

switch# traceroute 10.0.10.1 maxttl 20 timeout 5 minttl 1 probes 3 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 5 sec. timeout, 3
probes
 1 10.0.40.2 0.002ms 0.002ms 0.001ms
```

```

2 10.0.30.1 0.002ms 0.001ms 0.001ms
3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute 10.0.10.1 ip-option loosesourceroute 10.0.40.2
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 30 hops max, 3 sec. timeout, 3
probes
1 10.0.40.2 0.002ms 0.002ms 0.001ms
2 10.0.30.1 0.002ms 0.001ms 0.001ms
3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute 10.0.10.1 ip-option loosesourceroute 10.0.40.2 maxttl 20
timeout 5 minttl 1 probes 3 dstport 33434
traceroute to 10.0.10.1 (10.0.10.1) , 1 hops min, 20 hops max, 5 sec. timeout, 3
probes
1 10.0.40.2 0.002ms 0.002ms 0.001ms
2 10.0.30.1 0.002ms 0.001ms 0.001ms
3 10.0.10.1 0.001ms 0.002ms 0.002ms

switch# traceroute 10.0.0.2 source 10.0.0.1
traceroute to 10.0.0.2 (10.0.0.2), 30 hops max
1 10.0.0.2 0.299ms 0.155ms 0.115ms

switch# traceroute 10.0.0.2 source 1/1/1
traceroute to 10.0.0.2 (10.0.0.2), 30 hops max
1 10.0.0.2 0.479ms 0.222ms 0.171ms

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification                                                  |
|------------------|---------------------------------------------------------------|
| 10.08            | Added source IP address and source interface name parameters. |
| 10.07 or earlier | --                                                            |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## traceroute6

```
traceroute6 {<IPv6-ADDR> | <HOSTNAME>} [dstport <NUMBER> | maxttl <NUMBER> | probes
<NUMBER> | timeout <TIME>] [vrf <VRF-NAME>] source {<IPv6-ADDR> | <IFNAME>}
```

## Description

Uses traceroute for the specified IPv6 address or hostname with or without optional parameters.

| Parameter                       | Description                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------|
| IPv6-address <IPV6-ADDR>        | Specifies the IPv6 address.                                                         |
| hostname                        | Specifies the hostname of the device to traceroute.                                 |
| dstport <NUMBER>                | Specifies the destination port, <1-34000>. Default: 33434                           |
| maxttl <NUMBER>                 | Specifies the maximum number of hops to reach the destination, <1-255>. Default: 30 |
| probes <NUMBER>                 | Specifies the number of probes, <1-5>. Default: 3                                   |
| timeout <TIME>                  | Specifies the traceroute timeout in seconds, <1-60>. Default: 3 seconds             |
| vrf <VRF-NAME>                  | Specifies the virtual routing and forwarding (VRF) to use, <VRF-NAME>.              |
| source {<IPV6-ADDR>   <IFNAME>} | Specifies the source IPv6 address or interface name.                                |

## Usage

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays of packets across an Internet Protocol (IP) network. It sends a sequence of User Datagram Protocol (UDP) packets addressed to a destination host. The time-to-live (TTL) value, also known as hop limit, is used in determining the intermediate routers being traversed towards the destination.

## Examples

```
switch# traceroute6 0:0::0:1
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms

switch# traceroute6 localhost
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.089 ms 0.03 ms 0.014 ms

switch# traceroute6 0:0::0:1 maxttl 30
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms

switch# traceroute6 0:0::0:1 dstport 33434
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms

switch# traceroute6 0:0::0:1 probes 2
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 2 probes, 24
byte packets
 1 localhost (::1) 0.117 ms 0.032 ms

switch# traceroute6 0:0::0:1 timeout 3
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms
```

```

switch# traceroute6 localhost vrf red
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.077 ms 0.051 ms 0.054 ms

switch# traceroute6 localhost mgmt
traceroute to localhost (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.089 ms 0.03 ms 0.014 ms

switch# traceroute6 0:0::0:1 maxttl 30 timeout 3 probes 3 dstport 33434
traceroute to 0:0::0:1 (::1) from ::1, 30 hops max, 3 sec. timeout, 3 probes, 24
byte packets
 1 localhost (::1) 0.117 ms 0.032 ms 0.021 ms

switch# traceroute6 2001::2 source 2001::1
traceroute to 2001::2 (2001::2) from 2001::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
 1 2001::2 (2001::2) 0.4331 ms 0.3186 ms 0.1874 ms

switch# traceroute6 2001::2 source 1/1/1
traceroute to 2001::2 (2001::2) from 2001::1, 30 hops max, 3 sec. timeout, 3
probes, 24 byte packets
 1 2001::2 (2001::2) 0.6145 ms 0.4165 ms 0.1620 ms

```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification                                                                |
|------------------|-----------------------------------------------------------------------------|
| 10.08            | Added <b>source IP address</b> and <b>source interface name</b> parameters. |
| 10.07 or earlier | --                                                                          |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

### monitor type

```
monitor <MONITOR-NAME> type <FLOW-TYPE>
 entries <NUM>
 running-statistics-timeout <NUM>
 group-by dstip|dstport|ipproto|srcip|srcport|srcip_dstport|srcip_appid|
 filter-by {src_ip_mask <string>}|{dst_ip_mask <string>}|{src_ip <string>}|{dst_ip
 <string>}|{src_port <string>}|{dst_port <string>}|{ip_proto <string>}|
```

#### Description

Enables flow monitoring on a traffic insight instance. A traffic insight instance consists of one or more flow monitor types.

#### Parameters

| Parameter                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <MONITOR-NAME>                         | Specifies the name of the monitor. Length: 3 to 80 alphanumeric characters, including underscore (_).                                                                                                                                                                                                                                                                                                                                                                                  |
| <FLOW-TYPE>                            | Specifies the flow monitor type. See <b>Usage</b> for details on each supported flow type.                                                                                                                                                                                                                                                                                                                                                                                             |
| entries <NUM>                          | Specifies the number of entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| running-statistics-timeout <360-86400> | Configure a running-statistics reset timeout in seconds (Default: 600 seconds). TopN flow monitor report entries are updated every 5 minutes and entries are cleared after the running-statistics-timeout is expired. It is recommended to configure a running-statistics-timeout value in the range between 540 and 2700 seconds to avoid entries getting cleared within 1-2 minutes once a report is generated.                                                                      |
| group-by                               | Groups the monitored data based on the parameters specified. The parameters are as follows: <ul style="list-style-type: none"><li>▪ dstip: Group by Destination IP.</li><li>▪ dstport : Group by Destination Port.</li><li>▪ ipproto: Group by IP Protocol.</li><li>▪ srcip : Group by Source IP.</li><li>▪ srcport : Group by Source Port.</li><li>▪ srcip_dstip : Group by Source IP and Destination IP.</li><li>▪ srcip_dstport: Group by Source IP and Destination Port.</li></ul> |
| filter-by                              | Filters by the parameters specified. The parameters are as follows:                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <ul style="list-style-type: none"> <li>■ <code>dst_ip &lt;string&gt;</code>: Filter by Destination IP.</li> <li>■ <code>dst_ip_mask &lt;string&gt;</code>: Filter by Destination IP Mask.</li> <li>■ <code>dst_port &lt;string&gt;</code>: Filter by Destination Port.</li> <li>■ <code>ip_proto &lt;string&gt;</code>: Filter by IP Protocol. Supported options are <b>tcp</b>, <b>udp</b>, <b>icmp</b>, <b>ipv6-icmp</b></li> <li>■ <code>src_ip &lt;string&gt;</code>: Filter by Source IP.</li> <li>■ <code>src_ip_mask &lt;string&gt;</code>: Filter by Source IP Mask.</li> <li>■ <code>src_port &lt;string&gt;</code>: Filter by Source Port.</li> </ul> |

## Usage

The following flow monitor types are supported:

- **topN-flows**: Monitors IP traffic flowing through the switch and captures topN volume flows. The default number of top flows captured is 5. Running statistics are maintained for topN flows. By default running statistics are cleared for every 600 seconds. This flow monitor type is supported on 5420, 6200, 600, 6400, 8100, 8325, 8325H, 8325P, 8360, 9300, 9300S and 10000 Switch series.
  - A topN flow monitor caches flows up to 10 minutes to show total flow volume for last 10 minutes. The cache size will grow if there are many short-lived flows in the network. Do not set the running-statistics-timeout value to less than the default value (10 minutes) when there are many short lived flows in the network.
  - Memory usage can be high if multiple topN monitors are configured, so best practices to create no more than two topN monitors.
- **flow** - A workload-flows type monitor supported on 8100, 8325, 8325H, 8325P, 8360, 9300, 9300S and 10000 Switch series. A maximum of 1 flow monitor is allowed per traffic insight instance.
- **dropped-flows**: Monitors traffic flows that are dropped. If there are any dropped flows, the flow monitor shows the corresponding drop reasons sorted into groups, like L1, L2, L3 and MCAST. The Traffic-Insight Dropped-Flow table is updated once every 12 minutes, unless the flow count exceeds 1000 flows, at which point the table is updated every 30 seconds). A maximum of 1000 flows can be written to the database in a single update. This feature is supported on the 5420, 6200, 6300, 6400, 8100, 8325, 8325H, 8325P, 8360, and 9300 platforms.

## Examples

The following example configures **mntr1** with topN-flows:

```
switch(config-ti)# monitor mntr1 type topN-flows running-statistics-timeout 1800
switch(config-ti)# monitor mntr1 type topN-flows filter-by ipproto tcp
switch(config-ti)# monitor mntr2 type topN-flows group-by src_ip filter-by src_ip
mask 192.0.0.0/8
switch(config-ti)# monitor mntr1 type topN-flows entries 10
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                                                                                              |
|------------|-----------------------------------------------------------------------------------------------------------|
| 10.17      | The <b>dropped-flows</b> flow monitor type is available on 5420, 6200, 8100, 8360 and 9300 Switch series. |
| 10.16      | Command introduced on 5420, 8325H, 8325P, 9300 Switch series.                                             |
| 10.15.1000 | Command introduced on 8100, 8325, 8360, 9300S and 10000 Switch series.                                    |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-ti       | Administrators or local user group members with execution rights for this command. |

# show capacities traffic-insight

show capacities traffic-insight

## Description

Displays the system capacities status and their values for Traffic Insight.

## Examples

For 8100, 8360, 8325 ,8325P, 8325H, 9300S, 9300 switch series, the **show tech traffic-insight** command shows the following information:

```
switch# show capacities traffic-insight

System Capacities: Filter TRAFFIC_INSIGHT
Capacities Name Value

Maximum number of Traffic-insight flow table entries 2000
Maximum number of Traffic-insight flow cache entries 150000
Maximum number of Traffic-insight instances 1
Maximum number of Traffic-insight monitors 5
Maximum number of Traffic-insight TopN monitor reports 100
Maximum number of Traffic-insight TopN monitor reports per monitor 20
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification                                          |
|---------|-------------------------------------------------------|
| 10.16   | Support added for 5420, 9300 and 9300S Switch Series. |
| 10.11   | Command introduced.                                   |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show debug buffer module trafficinsight

show debug buffer module trafficinsight

### Description

Displays Traffic Insight debug logs stored in the debug buffer.

### Examples

```
Switch# show debug buffer module trafficinsight

show debug buffer

2022-10-26:11:11:30.689510|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|Unsupported record id: 210
2022-10-26:11:11:30.689573|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|DMAC: 10:4f:58:88:08:00
2022-10-26:11:11:30.689639|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|Unsupported record id: 210
2022-10-26:11:11:30.689700|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|octetDeltaCount: 13751
2022-10-26:11:11:30.689761|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|packetDeltaCount: 36
2022-10-26:11:11:30.689823|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|source interface: 0
2022-10-26:11:11:30.689887|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|Unsupported record id: 252
2022-10-26:11:11:30.689949|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT_PACKET|App id: 3235
2022-10-26:11:11:30.690159|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT|ti_recv_messages_in_cpdi_layer:
Received message with size 200 from DL
2022-10-26:11:11:30.690184|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT|ti_cpdi_layer_handle_events: Handling
message in CPDI event 10
2022-10-26:11:11:30.690321|traffic-insightd|LOG_
DEBUG|AMM|1/1|TRAFFICINSIGHT|TRAFFICINSIGHT|ti_topn_add_record_to_monitor:New TOPN
hash node created for SIP 3501::100, DIP 3701::100, VRF default,dst_port 80
```



For more information on features that use this command, refer to the Security Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.11   | Command introduced. |

### Command Information



| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show events traffic-insightd

`show events -d traffic-insightd`

### Description

Displays event logs generated by the switch modules since the last reboot for Traffic Insight.

### Examples

Showing event logs of Traffic Insight:

```
Switch# show events -d traffic-insightd

Event logs from current boot

2022-10-26T07:55:17.369208+00:00 6410 traffic-insightd[2518]: Event|14005|LOG_
INFO|UMM|-|Traffic Insight instance t1 enabled
2022-10-26T07:55:17.369309+00:00 6410 traffic-insightd[2518]: Event|14001|LOG_
INFO|UMM|-|Instance t1 created
```



For more information on features that use this command, refer to the Security Guide for your switch model.

### Command History

| Release    | Modification                            |
|------------|-----------------------------------------|
| 10.14.1000 | Command updated for 8325 Switch Series. |
| 10.11      | Command introduced.                     |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show running-config traffic-insight

`show running-config traffic-insight`

### Description

Display configuration settings for all traffic insight instances.

### Examples

Example **show running-config traffic-insight** output for 5420 ,6200, 6300, 6400, 8100, 8325, 8325P, 8325H, 8360, 9300, 9300S and 10000 Switch series:

```
switch(config-ti)# monitor mntr1 type topN-flows entries 20 group-by srcip_dstip
switch# show running-config traffic-insight
traffic-insight ti
enable
source ipfix
!
monitor top-1 type topN-flows entries 20 group-by srcip_dstip
...
```



For more information on features that use this command, refer to the Application Traffic Visibility Guide for your switch model.

## Related Commands

| Command                         | Description                                     |
|---------------------------------|-------------------------------------------------|
| <a href="#">traffic-insight</a> | Create and configure a traffic insight instance |

## Command History

| Release    | Modification                            |
|------------|-----------------------------------------|
| 10.14.1000 | Command updated for 8325 Switch Series. |
| 10.11      | Command introduced.                     |

## Command Information

| Platforms             | Command context                | Authority                                                                             |
|-----------------------|--------------------------------|---------------------------------------------------------------------------------------|
| 8360<br>9300<br>9300S | Operator (>) or<br>Manager (#) | Administrators or local user group members with<br>execution rights for this command. |

# show tech traffic-insight

```
show tech traffic-insight
```

## Description

Shows the Traffic Insight configuration settings as displayed in the output of the **show running-config traffic-insight** command..

## Examples

The following example shows possible output for the **show tech traffic-insight** command. The output of this command will vary, depending upon the traffic insight feature options available for each switch model and the traffic insight configuration.

```

Switch# show tech traffic-insight
=====
Show Tech executed on Wed Oct 26 11:11:37 2022
=====
[Begin] Feature traffic-insight
=====

Command : show running-config traffic-insight

traffic-insight t1
enable
source ipfix
!
monitor top4 type topN-flows entries 20 group-by srcip
=====
[End] Feature traffic-insight
=====
Show Tech commands executed successfully
=====

```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release    | Modification                            |
|------------|-----------------------------------------|
| 10.14.1000 | Command updated for 8325 Switch Series. |
| 10.11      | Command introduced.                     |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show traffic-insight monitor-type

```

show traffic-insight <INSTANCE_NAME> monitor-type
 flow <MONITOR_NAME> [vrf {<VRF_NAME>|all}] [permitted|denied|dropped|forwarded]
 topN-flows <MONITOR_NAME>}all

```

## Description

Display information for traffic insight monitored flows.

| Parameter       | Description                                                                         |
|-----------------|-------------------------------------------------------------------------------------|
| <INSTANCE_NAME> | Name of the traffic insight instance, string of maximum length up to 32 characters. |

| Parameter                            | Description                                                                                                                                                                                                                                                                          |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| flow <MONITOR_NAME>                  | Displays details for the specified <b>flow</b> type monitor.                                                                                                                                                                                                                         |
| vrf {<VRF_NAME> all}                 | Show traffic for the specified VRF, or use the <b>all</b> parameter to display information for all VRFs.                                                                                                                                                                             |
| denied                               | Show denied traffic insight flows only.                                                                                                                                                                                                                                              |
| dropped                              | Show dropped traffic insight flows only.                                                                                                                                                                                                                                             |
| forwarded                            | Show forwarded traffic insight flows only.                                                                                                                                                                                                                                           |
| permitted                            | Show permitted traffic insight flows only.                                                                                                                                                                                                                                           |
| permitted                            | Show denied flows for this application-flows monitor. This parameter is available on 5420, 6200, 6300, and 6400 Switch series.                                                                                                                                                       |
| denied                               | Show denied flows for this application-flows monitor. This parameter is available on 5420, 6200, 6300, and 6400 Switch series.                                                                                                                                                       |
| tls-visibility [client <CLIENT_MAC>] | Show TLS attributes for traffic insight flows. Include the optional <b>client</b> <CLIENT_MAC> parameter with a MAC address in <b>xx:xx:xx:xx:xx:xx</b> format to display details for a specific client only. This parameter is available on 5420, 6300 and 6400 Switch series only. |
| tls-cert-visibility                  | Show TLS certificate attributes for traffic insight flows. This parameter is available on 5420, 6300 and 6400 Switch series only.                                                                                                                                                    |
| forwarded                            | Show only forwarded flows. This parameter is available on 5420, 6300 and 6400 Switch series only.                                                                                                                                                                                    |
| dropped                              | Show only dropped flows. This parameter is available on 5420, 6300 and 6400 Switch series only.                                                                                                                                                                                      |
| interface-queue                      | Show traffic insight flows with interface and queue details for permitted flows. This parameter is available on 5420, 6300 and 6400 Switch series only.                                                                                                                              |
| dropped-flows                        | Display dropped flows information collected by a <b>dropped-flows</b> type traffic monitor.                                                                                                                                                                                          |
| <MONITOR_NAME> all                   | Specifies traffic insight monitor name. Choose <b>all</b> to display information for all monitors.                                                                                                                                                                                   |
| topN-flows                           | Display information collected by a <b>topN-flows</b> type traffic monitor.                                                                                                                                                                                                           |
| vrf                                  | Displays flows for a specific VRF.                                                                                                                                                                                                                                                   |
| <VRF-NAME> all                       | Specifies a valid VRF name.                                                                                                                                                                                                                                                          |

## Monitor types supported on different platforms

| Monitor type                              | Supported platforms                                             |
|-------------------------------------------|-----------------------------------------------------------------|
| application-flows                         | 5420/6200/6300/6400                                             |
| dns-average-latency                       | 5420/6300/6400 /8360                                            |
| dns-onboarding-latency                    | 5420/6300/6400                                                  |
| dropped-flows                             | 5420/6200/6300/6400/8100/8325/8325P/8360/9300                   |
| flow                                      | 8100/8325/8325H/8325P/8360/9300/9300S/10000                     |
| raw-flows                                 | 5420/6200/6300/6400                                             |
| topN-flows                                | 5420/6200/6300/6400/8100/8325/8325H/8325P/8360/9300/9300S/10000 |
| flows (formerly known as work-load-flows) | 10000                                                           |
| congested-flows                           | 5420/6200/6300/6400/8100/8360                                   |

## Examples

The following example shows **all** monitoring flow data for **topN-flows**, for instance **instance-1**:

```
switch# show traffic-insight instance-1 monitor-type topN-flows all
```

```
Name : top-5-dst-ip
Entries : 5
group By : dst_ip
Filter By : None
Running Statistics Timeout: 2700
```

```
Dataset : Running Statistics
```

| Rank | dst_ip          | Bytes |
|------|-----------------|-------|
| 1    | 34.94.235.109   | 4168  |
| 2    | 61.113.171.176  | 3500  |
| 3    | 41.244.240.249  | 3120  |
| 4    | 40.159.33.244   | 3084  |
| 5    | 247.182.130.159 | 3084  |

```
Name : top-5-conversations
Entries : 5
group By : dst_ip
Filter By : None
Running Statistics Timeout: 2700
```

```
Dataset: Running Statistics
```

| Rank | src_ip       | dst_ip          | ip_proto | src_port | dst_port | Bytes |
|------|--------------|-----------------|----------|----------|----------|-------|
| 1    | 192.168.1.6  | 223.126.110.198 | 17       | 18251    | 38530    | 102   |
| 2    | 11.89.15.20  | 143.193.61.233  | 17       | 43482    | 5929     | 103   |
| 3    | 107.56.36.77 | 255.111.58.122  | 6        | 15820    | 59117    | 104   |
| 4    | 1000::1      | 2000::2         | 6        | 20065    | 53239    | 105   |
| 5    | 3000::3      | 5000::5         | 17       | 12124    | 50782    | 105   |

The following example shows **top-5-dst-ip** monitoring flow data for **topN-flows**, for instance **instance-1**:

```
switch# show traffic-insight instance-1 monitor-type topN-flows top-5-dst-ip

Name : top-5-dst-ip
Entries : 5
group By : dst_ip
Filter By : None
Running Statistics Timeout: 2700

Dataset: Running Statistics

Rank dst_ip Bytes

1 34.94.235.109 4168
2 61.113.171.176 3500
3 41.244.240.249 3120
4 40.159.33.244 3084
5 247.182.130.159 3084
```

The following example shows an unconfigured traffic insight instance:

```
switch# show traffic-insight test monitor-type flow mon1

Traffic insight instance test is not configured
```



---

When instance is not configured an error message will be displayed.

---

The following example shows **all** monitoring flow data permitted or denied for **flows**, for monitor **mon1** on the 9300S switch series:

```
switch# show traffic-insight test monitor-type flow mon1 all

Name : mon1
Type : flow

VRF : default

src_mac : 00:00:00:00:00:00 dst_mac :
00:00:00:00:00:00

src_ip : 172.20.0.2 dst_ip : 172.40.0.2
src_vlan : VLAN100
src_port : 8000 dst_port : 20000
tx(bytes) : 1440 rx(bytes) : 1865
policy_type : NA policy_name : NA
class_name : NA rule_name : NA
policy_action : permitted forwarding_status : forwarded

VRF : Red

src_mac : aa:aa:aa:aa:aa:aa dst_mac :
```

```

bb:bb:bb:bb:bb:bb
src_ip : 172.60.0.3 dst_ip : 172.40.0.2
src_vlan : VLAN100
src_port : 8000 dst_port : 20000
tx(bytes) : 140 rx(bytes) : 18675
policy_type : vlan-acl policy_name : NA
class_name : acl1 rule_name : 0
policy_action : denied forwarding_status : dropped

```

For 8325, 8325P, 8325H, 8100, 8360, 9300, 9300S and 10000 Switch series the following example shows monitoring flow data collected by **topNflow** flow monitors :

```

show traffic-insight t1 monitor-type topN-flows top-monitor

Name : top-monitor
Group By : None
Entries : 5
Filter By : None
Running Statistics Timeout : 600

Dataset : Running Statistics
Rank dstip Bytes

1 37.1.1.15 84924695000
2 37.1.1.19 84923144678
3 37.1.1.16 84922587012
4 37.1.1.11 84922408979
5 36.1.1.18 84921561302

```

An error message displays when the traffic insight instance is not configured:

```

switch# show traffic-insight test monitor-type topN-flows mon1
Traffic insight instance test is not configured.

```

The following example shows traffic-insight data for on all VRFs collected on a flow monitor type on a 8100, 8325, 8325P, 8325H, 8360, 9300 or 9300S Switch series.

```

switch# show traffic-insight test monitor-type flow mon1 all

Name : mon1
Type : flow
VRF : default

src_mac : 00:50:56:96:05:e4 dst_mac : 00:50:56:96:c4:2e
src_ip : 10.0.0.2 dst_ip : 10.0.0.3
src_vlan : VLAN20
src_port : 53 dst_port : 85
tx(bytes) : 64 rx(bytes) : 0
policy_type : NA policy_name : NA
class_name : NA rule_name : NA
policy_action : permitted forwarding_status : forwarded

VRF : Red

src_mac : 00:50:56:96:05:e4 dst_mac : 00:50:56:96:c4:2e
src_ip : 10.0.0.2 dst_ip : 10.0.0.3
src_vlan : VLAN20
src_port : 53 dst_port : 85

```

```

tx(bytes) : 64
policy_type : NA
class_name : NA
policy_action : permitted

rx(bytes) : 0
policy_name : NA
rule_name : NA
forwarding_status : dropped

...

```



On the 9300S switch series, source MAC and destination MAC information is provided for denied flows but not for permitted flows, unless that information was obtained from a recently denied flow.



On the 8325, 8325H, 8325P, and 9300 Switch series, if collect ingress interface is not configured in the flow record, the VRF information will be invalid.

The following example shows denied traffic on the default VRF for a flow type traffic monitor on an 8100, 8325, 8325H, 8325P, 8360, 9300, or 9000S Switch series:

```

switch# show traffic-insight test monitor-type flow mon vrf default denied
Name : mon
Type : flow

VRF : default

src_mac : 00:50:56:96:75:6c dst_mac : 58:20:b1:bd:66:00
src_ip : 1.1.1.2 dst_ip : 2.2.2.2
src_vlan : VLAN10
src_port : 1001
tx(bytes) : 0
policy_type : port-acl
class_name : testacl
policy_action : denied

src_mac : 00:50:56:96:75:6c dst_mac : 58:20:b1:bd:66:00
src_ip : 1.1.1.2 dst_ip : 2.2.2.2
src_vlan : VLAN10
src_port : 1001
tx(bytes) : 0
policy_type : port-acl
class_name : testacl

dst_port : 101
rx(bytes) : 102
policy_name : NA
rule_name : 10
forwarding_status : dropped

dst_port : 106
rx(bytes) : 102
policy_name : NA
rule_name : 10

```



Policy-action for the flows is only based on Port-Access Role and Application Based Policing configurations.

The following example shows congested traffic when egress queues exceed their configured thresholds, on 5420, 6200, 6300, 6400, 8325, 8325P, 8325H and 9300-32D Switch series:

```

switch# show traffic-insight test monitor-type congested-flows mon
Name : mon
Type : congested-flows

src_ip : 10.10.10.1 dst_ip : 10.10.10.2
src_port : 1024
src_vlan : DEFAULT_VLAN_1
igrif : 1/1/1
dst_port : 22
protocol : 6
VRF : default

```



```
egrif : 1/1/2 egrq : 4 (80%)

Last Observed Congestion Events:
05/30/2024 21:06:05.400
05/30/2024 21:06:05.100
05/30/2024 21:06:04.369
```



The system displays up to the five most recent congestion events observed within the last 30 seconds.

The following example shows an error message displayed when monitor type is incorrect:

```
switch# show traffic-insight test monitor-type congested-flows mon1 all

Monitor mon1 type is not configured as congested-flows.
```

The following example shows an error message displayed when monitor name is incorrect:

```
switch# show traffic-insight test monitor-type congested-flows mon1 all

Monitor mon1 is not configured in traffic insight instance test.
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Related Commands

| Command                         | Description                                      |
|---------------------------------|--------------------------------------------------|
| <a href="#">traffic-insight</a> | Create and configure a traffic insight instance. |

## Command History

| Release | Modification                                    |
|---------|-------------------------------------------------|
| 10.17   | Introduces <b>congested-flows</b> monitor type. |
| 10.16   | Command introduced on the 9300cl switch series. |
| 10.15   | Command introduced on the 9300S switch series.  |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# traffic-insight

```

traffic-insight <INSTANCE_NAME>
 enable
 monitor <NAME> type
 flow
 topN-flows
 entries <Entry-VALUE>
 running-statistics-timeout <TIMEOUT-SECONDS>
 group-by <GROUP-TYPE>
 filter-by <FILTER-TYPE>
 no ...
 source ipfix
 traffic-insight flow-collector

```

## Description

Traffic insight monitors data collected from flow exporters like the IP Flow Information Export (IPFIX) flow exporter. Traffic insight tracks multiple monitor requests simultaneously and provides monitor reports for each request.



An egress Interface can be determined only after MAC and ARP resolution; the egress interface is exported only after next active/inactive timeout after the MAC entry is programmed. This is not applicable for 6200 Switch Series.

| Parameter                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INSTANCE_NAME>                              | Name of the traffic insight instance, string of maximum length up to 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| enable                                       | Use the <b>enable</b> parameter to enable this traffic insight configuration, or use the <b>no enable</b> option to disable traffic insight.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| monitor <INSTANCE_NAME> type                 | Enable flow monitoring on a traffic insight instance and configure rules for filtering and grouping traffic flows.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| flow                                         | Monitor traffic flows in the device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| topN-flows                                   | Monitors IP traffic flowing through the switch and captures topN flows volume. The default number of top flows captured is 5. This monitor type is available on all switches that support the traffic insight feature.                                                                                                                                                                                                                                                                                                                                                                                                              |
| entries <Entry-VALUE>                        | Select the maximum number of entries in the monitor report. Range: 1 to 20. The default value is 5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| running-statistics-timeout <TIMEOUT-SECONDS> | Sets running-statistics reset timeout value. Range: 360 to 86400. The default value is 600.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| filter-by <FILTER-TYPE>                      | Include any of the following values to filter the data set. <ul style="list-style-type: none"> <li>▪ <b>src_ip_mask &lt;IP_MASK&gt;</b>—Filter by source IP netmask</li> <li>▪ <b>dst_ip_mask &lt;IP_MASK&gt;</b>—Filter by destination IP netmask</li> <li>▪ <b>src_ip &lt;IP_ADDRESS&gt;</b>—Filter by source IP address</li> <li>▪ <b>dst_ip &lt;IP_ADDRESS&gt;</b>—Filter by destination IP address</li> <li>▪ <b>src_port &lt;PORT&gt;</b>—Filter by source port number</li> <li>▪ <b>dst_port &lt;PORT&gt;</b>—Filter by destination port number</li> <li>▪ <b>ip_proto &lt;PROTOCOL&gt;</b>—Filter by IP protocol</li> </ul> |

| Parameter                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             | <ul style="list-style-type: none"> <li>▪ <b>appid</b> &lt;string&gt;—Filter by application ID</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <code>group-by &lt;GROUP-TYPE&gt;</code>    | <p>Include any of the following values to create a monitor that groups matching traffic flows by that criteria.</p> <ul style="list-style-type: none"> <li>▪ <b>srcip</b>—Group by source IP address</li> <li>▪ <b>dstip</b> —Group by destination IP address</li> <li>▪ <b>srcport</b>—Group by source port number</li> <li>▪ <b>dstport</b>—Group by destination port number</li> <li>▪ <b>ipproto</b>—Group by IP protocol</li> <li>▪ <b>appid</b>—Group by application ID</li> <li>▪ <b>srcip_dstip</b>—Group by source IP and destination IP</li> <li>▪ <b>srcip_dstport</b>—Group by source IP and destination Port</li> <li>▪ <b>srcip_appid</b>—Group by source IP and application ID.</li> </ul> |
| <code>no ...</code>                         | Negate a command or reset it to default values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>source ipfix</code>                   | The traffic insight configuration uses this source protocol to collect traffic flows. The only available protocol is <b>ipfix</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>traffic-insight flow-collector</code> | Enables the Traffic insight flow collector on an IP interface. Traffic insight will listen for IPFIX packets destined for primary IP address of the port. The <b>no</b> form of the command disables traffic insight flow collector on the port.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Examples

The following example creates a traffic insight instance named **TI\_1**:

```
switch(config)# traffic-insight TI_1
```

The following example deletes a traffic insight instance named **TI\_1**:

```
switch(config)# no traffic-insight TI_1
```

The following example enables traffic insight instance for **TI\_1** instance:

```
switch(config)# traffic-insight TI_1
switch(config-ti)#enable
```

The following example disables traffic insight instance for **TI\_1** instance:

```
switch(config)# traffic-insight TI_1
switch(config-ti)#no enable
```

The following example sets the source protocol for **TI\_1** instance to collect flows information from IPFIX:

```
switch(config)# traffic-insight TI_1
switch(config-ti)# source ipfix
```

The following example removed the source protocol for **TI\_1** instance:

```
switch(config)# traffic-insight TI_1
switch(config-ti)# no source ipfix
```

The following examples create traffic insight monitor with filter and grouping rules for **topN-flows** for the **mnti1** monitoring:

```
switch(config)# traffic-insight TI_1
switch(config-ti)# monitor mnti1 type topN-flows
switch(config-ti)# monitor mnti1 type topN-flows running-statistics-timeout 1800
switch(config-ti)# monitor mnti1 type topN-flows group-by srcip
switch(config-ti)# monitor mnti1 type topN-flows filter-by src_ip_mask 192.0.0.0/8
```

The following example creates a traffic insight monitor with filter and grouping rules for **topN-flows** using the below parameter for the **mnti1** monitoring:

- 10 entries
- Grouped by **srcip** (Source IP)
- Filter by **src\_ip\_mask** (Source IP Mask)

```
switch(config-ti)# monitor mnti1 type topN-flows entries 10 group-by srcip filter-
by src_ip_mask 192.0.0.0/8
```

The following example removes flow monitoring:

```
switch(config)# traffic-insight TI_1
switch(config-ti)# no monitor mnti1 type topN-flows
```

The following example creates a traffic insight **monitor <NAME> type** for **topN flows** on a 9300, 9300S and 8325H Switch series:

```
switch(config)# monitor <NAME> type (topN-flows)
[entries <NUM> | running-statistics-timeout <NUM> |
group-by (srcip|dstip|srcport|dstport|ipproto|appid|srcip_dstip|
srcip_dstport|srcip_appid) |
filter-by (src_ip_mask STR | dst_ip_mask STR | src_ip STR |
dst_ip STR | src_port STR |dst_port STR |ip_proto STR
)
```

The following example creates a traffic insight **monitor <NAME>** for monitor type **flow on** 8100, 8325, 8325P, 8325H, 8360, 9300, 9300S or 10000 Switch series:



For more information on features that use this command, refer to the Security Guide for your switch model.

## Monitor types supported on different platforms

| Monitor type           | Supported platforms                                             |
|------------------------|-----------------------------------------------------------------|
| application-flows      | 5420/6200/6300/6400                                             |
| dns-average-latency    | 5420/6300/6400 /8360                                            |
| dns-onboarding-latency | 5420/6300/6400                                                  |
| dropped-flows          | 6300/6400 /8325/8325P                                           |
| flow                   | 8100/8325/8325H/8325P/8360/9300/9300S/10000                     |
| raw-flows              | 5420/6200/6300/6400                                             |
| topN-flows             | 5420/6200/6300/6400/8100/8325/8325H/8325P/8360/9300/9300S/10000 |
| workload-flows         | 10000                                                           |
| congested-flows        | 5420/6200/6300/6400/8100/8360                                   |

## Command History

| Release | Modification                                                                                                |
|---------|-------------------------------------------------------------------------------------------------------------|
| 10.17   | The <b>congested-flows</b> parameter is introduced for 5420, 6200, 6300, 6400, 8100 and 8360 switch series. |
| 10.16   | Command introduced on the 5420 and 9300 switch series.                                                      |
| 10.15   | Support added for 6200 and 9300S switches.                                                                  |
| 10.11   | Command introduced.                                                                                         |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# TLS commands

## cipher-suites 1.2 priority (TLS)

```

cipher-suites 1.2 priority <1-6> {tls-ecdhc-ecdsa-with-aes-256-gcm-sha384 |tls-ecdhc-ecdsa-with-aes-128-gcm-sha256 | tls-ecdhc-rsa-with-aes-256-gcm-sha384 | tls-ecdhc-rsa-with-aes-128-gcm-sha256 | tls-rsa-with-aes-256-gcm-sha384 | tls-rsa-with-aes-128-gcm-sha256 | none}
no priority <1-6> [tls-ecdhc-ecdsa-with-aes-256-gcm-sha384 |tls-ecdhc-ecdsa-with-aes-128-gcm-sha256 | tls-ecdhc-rsa-with-aes-256-gcm-sha384 | tls-ecdhc-rsa-with-aes-128-gcm-sha256 | tls-rsa-with-aes-256-gcm-sha384 | tls-rsa-with-aes-128-gcm-sha256 | none]
no cipher-suites 1.2

```

## Description

Configures TLS 1.2 cipher suites and their priority level. This configuration will be stored in the database and all applications using TLS 1.2 must consume this information to adhere to the configured TLS 1.2 cipher suite(s).

There is a cipher suite assigned by default to each priority:

- Priority 1: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- Priority 2: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- Priority 3: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- Priority 4: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- Priority 5: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- Priority 6: TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

If user assigns a cipher suite other than the default to a priority level or does not assign one at all then the default suite will not be applied unless it is assigned to another priority level. The removed cipher suite will not be used unless it is assigned to another priority level. To make a priority level have no assignment, the user must explicitly configure "none" for that priority level. Assignment of the same cipher suite to two priority levels is allowed, however it is considered a misconfiguration. When this misconfiguration occurs, the assignment to the higher priority level takes effect and the lower priority level is treated as unassigned (i.e., "none").

The two cipher suites involving ECDSA may be removed from client side offering by the underlying crypto library at runtime if signature algorithms are limited to RSA algorithms. That may happen on switches with TPM 1.2 and with device-identity certificate being used, where only signature algorithms sha256WithRSA, sha384WithRSA, and sha512WithRSA are allowed. In such situation, be sure to configure some TLS 1.2 cipher suites other than the ECDSA ones.

The **no** form of this command will reset all priority levels (or the specified level) to their default assignment. The removed cipher suite will not be applied until it is assigned to another priority level. If a priority level is already configured with its default suite, then using the **no** command on that priority level will have no effect.

| Parameter                                            | Description                                                                                                                        |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>priority &lt;1-6&gt;</code>                    | Selects the cipher suite priority level to be configured where 1 is the highest.                                                   |
| <code>tls-ecdhe-ecdsa-with-aes-256-gcm-sha384</code> | Specifies the <code>tls-ecdhe-ecdsa-with-aes-256-gcm-sha384</code> cipher suite to be associated with the selected priority level. |
| <code>tls-ecdhe-ecdsa-with-aes-128-gcm-sha256</code> | Specifies the <code>tls-ecdhe-ecdsa-with-aes-128-gcm-sha256</code> cipher suite to be associated with the selected priority level. |
| <code>tls-ecdhe-rsa-with-aes-256-gcm-sha384</code>   | Specifies the <code>tls-ecdhe-rsa-with-aes-256-gcm-sha384</code> cipher suite to be associated with the selected priority level.   |
| <code>tls-ecdhe-rsa-with-aes-128-gcm-sha256</code>   | Specifies the <code>tls-ecdhe-rsa-with-aes-128-gcm-sha256</code> cipher suite to be associated with the selected priority level.   |

| Parameter                                    | Description                                                                                                                |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <code>tls-rsa-with-aes-256-gcm-sha384</code> | Specifies the <code>tls-rsa-with-aes-256-gcm-sha384</code> cipher suite to be associated with the selected priority level. |
| <code>tls-rsa-with-aes-128-gcm-sha256</code> | Specifies the <code>tls-rsa-with-aes-128-gcm-sha256</code> cipher suite to be associated with the selected priority level. |
| <code>none</code>                            | Specifies no cipher suite assignment for the selected priority level.                                                      |

## Examples

Configuring `tls-ecdhc-ecdsa-with-aes-128-gcm-sha256` as the priority 4 cipher suite for TLS version 1.2:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.2
switch(config-tls-global-ciphers-1.2)# priority 4 tls-ecdhc-ecdsa-with-aes-128-gcm-sha256
```

Unconfiguring `tls-ecdhc-ecdsa-with-aes-128-gcm-sha256` as the priority 4 cipher suite for TLS version 1.2:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.2
switch(config-tls-global-ciphers-1.2)# no priority 4 tls-ecdhc-ecdsa-with-aes-128-gcm-sha256
```

Configuring no cipher suite associated with priority level 1 for TLS version 1.2:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.2
switch(config-tls-global-ciphers-1.2)# priority 1 none
```

Showing configured TLS 1.2 cipher suite priority levels in the running configuration:

```
switch(config)# show running-config tls global
tls global
 cipher-suites 1.2
 priority 1 none
 priority 2 tls-ecdhc-ecdsa-with-aes-128-gcm-sha256
 priority 3 tls-ecdhc-rsa-with-aes-256-gcm-sha384
 priority 4 tls-ecdhc-rsa-with-aes-128-gcm-sha256
 priority 5 tls-rsa-with-aes-256-gcm-sha384
 priority 6 tls-rsa-with-aes-128-gcm-sha256
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context                                                              | Authority                                                                          |
|---------------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config-tls-global</code><br><code>config-tls-global-ciphers-1.2</code> | Administrators or local user group members with execution rights for this command. |

## cipher-suites 1.3 priority

```
cipher-suites 1.3 priority <1-5> {tls-aes-256-gcm-sha384 | tls-aes-128-gcm-sha256 | tls-chacha20-poly1305-sha256 | tls-aes-128-ccm-8-sha256 | tls-aes-128-ccm-sha256 | none}
```

```
no priority <1-5> [tls-aes-256-gcm-sha384 | tls-aes-128-gcm-sha256 | tls-chacha20-poly1305-sha256 | tls-aes-128-ccm-8-sha256 | tls-aes-128-ccm-sha256 | none]
```

```
no cipher-suites 1.3
```

### Description

Configures TLS 1.3 cipher suites and their priority level. This configuration will be stored in the database and all applications using TLS 1.3 must consume this information to adhere to the configured TLS 1.3 cipher suite(s).

There is a cipher suite assigned by default to each priority:

- Priority 1: TLS\_AES\_256\_GCM\_SHA384
- Priority 2: TLS\_AES\_128\_GCM\_SHA256
- Priority 3: TLS\_CHACHA20\_POLY1305\_SHA256
- Priority 4: TLS\_AES\_128\_CCM\_8\_SHA256
- Priority 5: TLS\_AES\_128\_CCM\_SHA256

If user assigns a cipher suite other than the default to a priority level or does not assign one at all then the default suite will not be applied unless it is assigned to another priority level. The removed cipher suite will not be used unless it is assigned to another priority level. To make a priority level have no assignment, the user must explicitly configure "none" for that priority level. Assignment of the same cipher suite to two priority levels is allowed, however it is considered a misconfiguration. When this misconfiguration occurs, the assignment to the higher priority level takes effect and the lower priority level is treated as unassigned (i.e., "none").

Although FFDHE algorithms are in general usable with both TLS 1.2 and 1.3, the underlying crypto library may remove them from client side offering at runtime if only TLS 1.2 is allowed. If all TLS 1.3 cipher suite priorities are set to none, be sure to configure some key exchange algorithms other than the FFDHE ones.

The **no** form of this command will reset all priority levels (or the specified level) to their default assignment. The removed cipher suite will not be applied until it is assigned to another priority level. If a priority level is already configured with its default suite, then using the **no** command on that priority level will have no effect.



| Parameter                    | Description                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------|
| priority <1-5>               | Selects the cipher suite priority level to be configured where 1 is the highest.                                    |
| tls-aes-256-gcm-sha384       | Specifies the tls-aes-256-gcm-sha384 cipher suite to be associated with the selected priority level.                |
| tls-aes-128-gcm-sha256       | Specifies the tls-aes-128-gcm-sha256 cipher suite to be associated with the selected priority level.                |
| tls-chacha20-poly1305-sha256 | Specifies the tls-ecdhe-rsa-with-aes-256-gcm-sha384 cipher suite to be associated with the selected priority level. |
| tls-aes-128-ccm-8-sha256     | Specifies the tls-aes-128-ccm-8-sha256 cipher suite to be associated with the selected priority level.              |
| tls-aes-128-ccm-sha256       | Specifies the tls-aes-128-ccm-sha256 cipher suite to be associated with the selected priority level.                |
| none                         | Specifies no cipher suite assignment for the selected priority level.                                               |

## Examples

Configuring tls-aes-128-ccm-8-sha256 as the priority 2 cipher suite for TLS version 1.3:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.3
switch(config-tls-global-ciphers-1.3)# priority 2 tls-aes-128-ccm-8-sha256
```

Configuring tls-aes-128-ccm-sha256 as the priority 3 cipher suite for TLS version 1.3:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.3
switch(config-tls-global-ciphers-1.3)# priority 3 tls-aes-128-ccm-sha256
```

Unconfiguring tls-aes-128-ccm-8-sha256 as the priority 2 cipher suite for TLS version 1.3:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.3
switch(config-tls-global-ciphers-1.3)# no priority 2 tls-aes-128-ccm-8-sha256
```

Configuring no cipher suite associated with priority level 1 for TLS version 1.3:

```
switch(config)# tls global
switch(config-tls-global)# cipher-suites 1.3
switch(config-tls-global-ciphers-1.3)# priority 1 none
```

Showing configured TLS 1.3 cipher suite priority levels in the running configuration:

```
switch(config)# show running-config tls global
tls global
 cipher-suites 1.3
```

```
priority 1 none
priority 2 tls-aes-128-gcm-sha256
priority 3 tls-chacha20-poly1305-sha256
priority 4 tls-aes-128-ccm-8-sha256
priority 5 tls-aes-128-ccm-sha256
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context                                    | Authority                                                                          |
|---------------|----------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-tls-global<br>config-tls-global-ciphers-1.3 | Administrators or local user group members with execution rights for this command. |

## key-exchange-algorithms priority

```
key-exchange-algorithms priority <1-10> {secp521r1 | secp384r1 | secp256r1 | x25519 | x448
| ffdhe8192 | ffdhe6144 | ffdhe4096 | ffdhe3072 | ffdhe2048 | none}
```

```
no priority <1-10> [secp521r1 | secp384r1 | secp256r1 | x25519 | x448 | ffdhe8192 |
ffdhe6144 | ffdhe4096 | ffdhe3072 | ffdhe2048 | none]
```

```
no key-exchange-algorithms
```

## Description

Configures key exchange algorithms and their priority level. This configuration will be stored in the database and all applications which use TLS 1.2 or TLS 1.3 will consume this information to adhere to the configured key exchange algorithm(s).

There is a key exchange algorithm assigned by default to each priority:

- Priority 1: secp521r1
- Priority 2: secp384r1
- Priority 3: secp256r1
- Priority 4: X25519
- Priority 5: X448
- Priority 6: ffdhe8192
- Priority 7: ffdhe6144
- Priority 8: ffdhe4096
- Priority 9: ffdhe3072
- Priority 10: ffdhe2048

If user assigns a key exchange algorithm other than the default to a priority level or does not assign one at all then the default algorithm will not be applied unless it is assigned to another priority level. The removed algorithm will not be used unless it is assigned to another priority level. To make a priority level have no assignment, the user must explicitly configure "none" for that priority level. Assignment of the same algorithm to two priority levels is allowed, however it is considered a misconfiguration. When this misconfiguration occurs, the assignment to the higher priority level takes effect and the lower priority level is treated as unassigned (i.e., "none").

Although FFDHE algorithms are in general usable with both TLS 1.2 and 1.3, the underlying crypto library may remove them from client side offering at runtime if only TLS 1.2 is allowed. That happens on switches with TPM 1.2 where TLS 1.3 is not allowed, and on switches with all TLS 1.3 cipher suites are disallowed by users. In such situations, be sure to configure some key exchange algorithms other than the FFDHE ones.

The **no** form of this command will reset all priority levels (or the specified level) to their default assignment. The removed cipher suite will not be applied until it is assigned to another priority level. If a priority level is already configured with its default suite, then using the **no** command on that priority level will have no effect.

| Parameter                          | Description                                                                                       |
|------------------------------------|---------------------------------------------------------------------------------------------------|
| <code>priority &lt;1-10&gt;</code> | Selects the key exchange algorithm priority level to be configured where 1 is the highest.        |
| <code>secp521r1</code>             | Specifies the secp521r1 key exchange algorithm to be associated with the selected priority level. |
| <code>secp384r1</code>             | Specifies the secp384r1 key exchange algorithm to be associated with the selected priority level. |
| <code>secp256r1</code>             | Specifies the secp256r1 key exchange algorithm to be associated with the selected priority level. |
| <code>x25519</code>                | Specifies the x25519 key exchange algorithm to be associated with the selected priority level.    |
| <code>x448</code>                  | Specifies the x448 key exchange algorithm to be associated with the selected priority level.      |
| <code>ffdhe8192</code>             | Specifies the ffdhe8192 key exchange algorithm to be associated with the selected priority level. |
| <code>ffdhe6144</code>             | Specifies the ffdhe6144 key exchange algorithm to be associated with the selected priority level. |
| <code>ffdhe4096</code>             | Specifies the ffdhe4096 key exchange algorithm to be associated with the selected priority level. |
| <code>ffdhe3072</code>             | Specifies the ffdhe3072 key exchange algorithm to be associated with the selected priority level. |
| <code>ffdhe2048</code>             | Specifies the ffdhe2048 key exchange algorithm to be associated with the selected priority level. |
| <code>none</code>                  | Specifies no key exchange algorithm assignment for the selected priority level.                   |

## Examples

Configuring x25519 as the priority 1 key exchange algorithm:

```
switch(config)# tls global
switch(config-tls-global)# key-exchange-algorithms
switch(config-tls-global-key-ex-algo)# priority 1 x25519
```

Configuring ffdhe2048 as the priority 2 key exchange algorithm:

```
switch(config)# tls global
switch(config-tls-global)# key-exchange-algorithms
switch(config-tls-global-key-ex-algo)# priority 2 ffdhe2048
```

Unconfiguring ffdhe2048 as the priority 2 key exchange algorithm:

```
switch(config)# tls global
switch(config-tls-global)# key-exchange-algorithms
switch(config-tls-global-key-ex-algo)# no priority 2 ffdhe2048
```

Configuring priority 3 with no key exchange algorithm. This will disallow the algorithm that was previously assigned to priority 3 unless it has already been assigned to another priority level:

```
switch(config)# tls global
switch(config-tls-global)# key-exchange-algorithms
switch(config-tls-global-key-ex-algo)# priority 3 none
```

Showing the configured key exchange algorithm priority levels in the running configuration:

```
(config)# show running-config tls global
tls global
 key-exchange-algorithms
 priority 1 secp521r1
 priority 2 secp384r1
 priority 3 none
 priority 4 x25519
 priority 5 x448
 priority 6 ffdhe8192
 priority 7 ffdhe6144
 priority 8 ffdhe4096
 priority 9 ffdhe3072
 priority 10 ffdhe2048
```



---

For more information on features that use this command, refer to the Security Guide for your switch model.

---

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context                                    | Authority                                                                          |
|---------------|----------------------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-tls-global<br>config-tls-global-key-ex-algo | Administrators or local user group members with execution rights for this command. |

## min-version

```
min-version {1.2|1.3}
no min-version [1.2|1.3]
```

### Description

Configures the minimum TLS version to be supported by TLS applications. Default is TLS 1.2.

The setting of a minimum version indicates the system allows this version and all versions above.

On a switch that uses a TPM of legacy version 1.2, the device-identity certificate is only compatible with TLS 1.2.

Setting the minimum version higher than 1.2 from the CLI will be rejected when the device-identity certificate has been associated with an application. Attempting such a configuration through REST will make the certificate association invalid and local-cert will be used for the affected applications instead.

On a TPM 1.2 switch with TLS minimum version of 1.2 and a client application associated with device-identity certificate, the client will be limited to sha256WithRSA, sha384WithRSA, and sha512WithRSA for signature algorithms. The underlying crypto library may remove the cipher suites involving ECDSA from the client side offering at runtime even if such cipher suites are allowed in user configuration.

The **no** version of this command resets the minimum version back to its default value of TLS 1.2.

| Parameter | Description                                    |
|-----------|------------------------------------------------|
| 1.2       | Specifies TLS versions 1.2 and above. Default. |
| 1.3       | Specifies TLS versions 1.3 and above.          |

### Examples

Configuring the switch to use TLS versions 1.3 and above:

```
switch(config)# tls global
switch(config-tls-global)# min-version 1.3
```

Unconfiguring the TLS minimum version:

```
switch(config)# tls global
switch(config-tls-global)# no min-version
```



For more information on features that use this command, refer to the Security Guide for your switch model.

### Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context   | Authority                                                                          |
|---------------|-------------------|------------------------------------------------------------------------------------|
| All platforms | config-tls-global | Administrators or local user group members with execution rights for this command. |

# tls global

tls global

## Description

Enters the TLS global configuration context allowing the user to configure global TLS configuration settings.

## Examples

Entering the TLS global configuration context:

```
switch(config)# tls global
switch(config-tls-global)#
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# show tls

show tls global

## Description

Shows the TLS global operational state in effect.

## Examples

## Showing Transport Layer Security (TLS) information:

```
switch(config)# show tls global
Minimum TLS version : 1.2

TLS 1.2 cipher suites from highest to lowest priority :
State Cipher Suite

allowed TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
allowed TLS_RSA_WITH_AES_256_GCM_SHA384
allowed TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
disallowed TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
disallowed TLS_RSA_WITH_AES_128_GCM_SHA256
disallowed TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS 1.3 cipher suites from highest to lowest priority :
State Cipher Suite

allowed TLS_AES_256_GCM_SHA384
allowed TLS_CHACHA20_POLY1305_SHA256
disallowed TLS_AES_128_GCM_SHA256
disallowed TLS_AES_128_CCM_8_SHA256
disallowed TLS_AES_128_CCM_SHA256

TLS key exchange algorithms from highest to lowest priority :
State Algorithm

allowed secp384r1
allowed ffdhe8192
allowed ffdhe6144
disallowed ffdhe2048
disallowed ffdhe3072
disallowed X25519
disallowed X448
disallowed secp256r1
disallowed secp521r1
disallowed ffdhe4096

switch(config)# tls global
switch(config-tls-global)# min-version 1.3
switch(config-tls-global)# exit
switch(config)# show tls global

Minimum TLS version : 1.3

TLS 1.3 cipher suites from highest to lowest priority :
State Cipher Suite

allowed TLS_AES_256_GCM_SHA384
allowed TLS_CHACHA20_POLY1305_SHA256
disallowed TLS_AES_128_GCM_SHA256
disallowed TLS_AES_128_CCM_8_SHA256
disallowed TLS_AES_128_CCM_SHA256

TLS key exchange algorithms from highest to lowest priority :
State Algorithm

allowed secp384r1
allowed ffdhe8192
allowed ffdhe6144
disallowed ffdhe2048
disallowed ffdhe3072
disallowed X25519
```

```
disallowed X448
disallowed secp256r1
disallowed secp521r1
disallowed ffdhe4096
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.16   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |



## Two-factor authentication commands

### aaa authorization radius

```
aaa authorization radius {ssh | https-server} group <GROUP-LIST>
no aaa authorization radius {ssh | https-server} group <GROUP-LIST>
```

#### Description

Enables RADIUS authorize-only for use with two-factor authentication. By default RADIUS authenticates and authorizes a client that is configured for AAA based access. This command causes the RADIUS server to instead be used only for authorization and not for authentication.

Authorization requests are sent over TLS and therefore RADIUS authorize-only requires a RadSec RADIUS server.



If command authorization is also configured it is given priority over RADIUS authorize-only and therefore command authorization is done on the basis of command authorization configuration and not the user role and privilege level assigned by the RADIUS server.

The **no** form of this command disables RADIUS authorize-only, causing RADIUS to be again used for both authentication and authorization.

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssh                | Selects the SSH authorization list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| https-server       | Selects the HTTPS server authorization list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| group <GROUP-LIST> | Specifies the list of remote RADIUS server group names. Each name can be specified one time. Predefined remote RADIUS group name <b>radius</b> is available.<br>The remote RADIUS server groups are accessed in the order that the group names are listed in this command. Within each group, the servers are accessed in the order in which the servers were added to the group. Server groups are defined using command <b>aaa group server</b> and servers are added to a server group with the command <b>server</b> . |

#### Examples

Enabling RADIUS authorize only for SSH with the default RADIUS group:

```
switch(config)# aaa authorization radius ssh group radius
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y
```

Disabling RADIUS authorize only for SSH with the default RADIUS group, causing RADIUS to be again used for both authentication and authorization:

```
switch(config)# no aaa authorization radius ssh group radius
```

Enabling RADIUS authorize only for HTTPS server with the default RADIUS group:

```
switch(config)# aaa authorization radius https-server group radius
All commands will fail if none of the radsec servers in the group list are
reachable.
Continue (y/n)? y
```

Disabling RADIUS authorize only for HTTPS server with the default RADIUS group, causing RADIUS to be again used for both authentication and authorization:

```
switch(config)# no aaa authorization radius https-server group radius
```



For more information on features that use this command, refer to the Security Guide for your switch model.

| Release | Modification       |
|---------|--------------------|
| 10.11   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## https-server authentication certificate

```
https-server authentication certificate [authorization radius] [username {<CERT-FIELD>}]
```

### Description

Enables certificate-based authentication where the HTTPS server uses an X.509 certificate for authentication and a RADIUS server for authorization.

Enabling password authentication is the only way of disabling certificate authentication.

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authorization radius | Specifies that after certificate authentication succeeds, instead of prompting for a password, the HTTPS server checks the RADIUS server only for authorization. A local user is not required.<br>By default, the username found in the certificate field UserPrincipalName (UPN) is used for authorization on the RADIUS server.<br>When this parameter is omitted, <b>authorization radius</b> is still the assumed active setting. |

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;CERT-FIELD&gt;</code> | <p>Selects which certificate username field is to be used for authorization.</p> <ul style="list-style-type: none"> <li>Specify <b>user_principal_name</b> to use the certificate UserPrincipalName (UPN) field. This is the default.</li> <li>Specify <b>common_name</b> to use the certificate CommonName (CN) field.</li> </ul> <p>When this parameter is omitted, <b>user_principal_name</b> is assumed.</p> |

## Examples

Enabling HTTPS server authentication with authorization on a RADIUS server with the username in certificate field UserPrincipalName (UPN):

```
switch(config)# https-server authentication certificate authorization radius
```

Enabling HTTPS server authentication with authorization on a RADIUS server with the username in certificate field UserPrincipalName (UPN) (**authorization radius** is still implied even though not specified):

```
switch(config)# https-server authentication certificate
```

Enabling HTTPS server authentication with authorization on a RADIUS server with the username in certificate field CommonName (CN):

```
switch(config)# https-server authentication certificate authorization radius
username common_name
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.11   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ssh certificate-as-authorized-key

```
ssh certificate-as-authorized-key
no ssh certificate-as-authorized-key
```

## Description

Enables SSH enforcement that the username must be present in the certificate that is being used for authorization. This configuration alters how certificate-based authentication maps to a user account. When this is enabled, SSH will not require local user association with an authorized-key and instead enforces that the username used to log in is present within the certificate.

The SSH server will check for the username in certificate fields **Common Name** or **User Principle Name** for a match. If a certificate is not used for authentication then this configuration has no effect on SSH authentication.

The **no** form of this command disables the SSH enforcement of username in the certificate.

## Examples

Enabling SSH enforcement of username in the certificate:

```
switch(config)# ssh certificate-as-authorized-key
```

Disabling SSH enforcement of username in the certificate:

```
switch(config)# no ssh certificate-as-authorized-key
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.11   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ssh two-factor-authentication

```
ssh two-factor-authentication [authorization radius]
no ssh two-factor-authentication [authorization radius]
```

### Description

Enables the selected SSH Two Factor authentication method. Two-factor authentication uses an X.509 certificate and possibly a password. First the X.509 certificate presented by the user is authenticated. Then, if successful, (when the **authorization-radius** parameter is not specified) the (locally-defined) user is prompted for a password. When the **authorization radius** parameter is specified, instead of prompting for a password, SSH checks only for authorization with the remote RADIUS server. A local user is not required.

The **no** form of the command disables SSH two-factor authentication.

| Parameter                         | Description                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------|
| <code>authorization radius</code> | Specifies that after certificate authentication succeeds, SSH checks the RADIUS server only for authorization. |

## Examples

Enabling two-factor authentication for local user with password prompting:

```
switch(config)# ssh two-factor-authentication
```

Disabling two-factor authentication for local user with password prompting:

```
switch(config)# no ssh two-factor-authentication
```

Enabling two-factor authentication for remote-only RADIUS-defined users without password prompting:

```
switch(config)# ssh two-factor-authentication authorization radius
```

Disabling two-factor authentication for remote-only RADIUS-defined users without password prompting: :

```
switch(config)# no ssh two-factor-authentication authorization radius
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification                                    |
|---------|-------------------------------------------------|
| 10.11   | Added the <b>authorization radius</b> parameter |
| 10.10   | Command introduced                              |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## clear udld statistics

clear udld statistics [interface <INTERFACE-NAME>]

### Description

Clears UDLD statistics for all interfaces or a specific interface.

### Examples

Clearing all UDLD statistics on all interfaces:

```
switch# clear udld statistics
```

Clearing all UDLD statistics on interface 1/1/1:

```
switch# clear udld statistics interface 1/1/1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show udld

show udld [interface <INTERFACE-NAME>] [vsx-peer]

### Description

Displays UDLD information for all interfaces or for a specific interface.

| Parameter                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>interface &lt;INTERFACE-NAME&gt;</code> | Specifies the name of a logical interface on the switch, which can be: <ul style="list-style-type: none"> <li>An Ethernet interface associated with a physical port. Use the format <b>member/slot/port</b> (for example, <b>1/3/1</b>).</li> <li>UDLD runs only on physical interfaces. LAGs, tunnels, and the like are not supported. However, UDLD can be configured individually on each port of a LAG or trunk group. Configuring UDLD on a trunk group primary port enables UDLD on that port only.</li> </ul> |
| <code>vsx-peer</code>                         | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                                                                                                                                                                                                                                                                     |

## Examples

Displaying all UDLD information:

```
switch# show udld
```

Abbreviations:  
VTF - Verify-then-forward      FTV - Forward-then-verify  
NOR - RFC 5171 normal          AGG - RFC 5171 aggressive

| Interface | UDLD Config | UDLD State | UDLD Substate | UDLD Link | Mode | Interval |
|-----------|-------------|------------|---------------|-----------|------|----------|
| 1/1/1     | Disabled    | Inactive   | Undetermined  | Unblock   | FTV  | 8000     |
| 1/1/2     | Enabled     | Active     | Bidirectional | Unblock   | FTV  | 7000     |
| 1/1/3     | Enabled     | Active     | Blocked       | Block     | FTV  | 7000     |
| 1/1/4     | Enabled     | Inactive   | Uninitialized | Unblock   | NOR  | 7000     |
| 1/1/5     | Enabled     | Active     | ErrDisabled   | Block     | AGG  | 7000     |
| 1/1/6     | Disabled    | Active     | Detection     | Unblock   | NOR  | 7000     |

| Retries | Tx Pkts | Rx Pkts | Rx Pkts disc. | Rx Pkts drop. | Transitions |
|---------|---------|---------|---------------|---------------|-------------|
| 4       | 4       | 54      | 123           | 123           | 1           |
| 7       | 1234567 | 1548421 | 23214         | 1878981       | 3           |
| 4       | 3       | 77871   | 2157          | 81878         | 1           |
| 5       | 50      | 0       | 0             | 0             | 0           |
| 3       | 150     | 25      | 0             | 2             | 1           |
| 3       | 6       | 54      | 123           | 23            | 1           |

Displaying information for interface **1/1/1**:

```
switch# show udld interface 1/1/1
```

```
Interface 1/1/1
Config: Enabled
State: Active
Substate: Bidirectional
```

```

Link: Unblock
Mode: Forward then verify
Interval: 7000 milliseconds
Retries: 7
Tx: 1234567 packets
Rx: 1548421 packets, 23214 discarded packets, 1878981 dropped packets
Port transitions: 3

```

Displaying the UDLD enable interfaces information:

```
switch# show udld enabled
```

Abbreviations:

```

VTF - Verify-then-forward FTV - Forward-then-verify
NOR - RFC 5171 normal AGG - RFC 5171 aggressive

```

```

Interface UDLD UDLD UDLD UDLD Mode Interval Retries Tx
 Rx Rx Rx Substate Transitions
 Pkts Config State Pkts drop. Link

2 Enabled Active Bidirectional Unblock FTV 7000 7
1234567 1548421 23214 1878981 3
3 Enabled Active Blocked Block FTV 7000 4 3
 77871 2157 81878 1
4 Enabled Inactive Uninitialized Unblock NOR 7000 5 50
 0 0 0 0
5 Enabled Active ErrDisabled Block AGG 7000 3
150 25 0 2 1

```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## udld

```

udld [disable]
no udld [disable]

```



## Description

Enables UDLD support on a physical interface. UDLD is disabled by default. UDLD is configured on a per-port basis and must be enabled at both ends of the link.

UDLD runs only on physical interfaces. LAGs, tunnels, and the like are not supported. However, UDLD can be configured individually on each port of a LAG or trunk group. Configuring UDLD on a trunk group's primary port enables UDLD on that port only.

The **no** form of this command disables UDLD support and resets all configuration values to their default settings.

| Parameter      | Description                                                                 |
|----------------|-----------------------------------------------------------------------------|
| <i>disable</i> | Disables UDLD on the interface but retains all UDLD configuration settings. |

## Examples

Enabling UDLD on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# udld
```

Disabling UDLD on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no udld
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## udld interval

```
udld interval <TIME>
no udld interval [<TIME>]
```

## Description

Sets the packet transmission interval.

The **no** form of this command sets the packet transmission interval to the default value of 7000 ms.

The allowed values vary depending on the operation mode.

The default interval is 7000 ms (7 seconds) for both ArubaOS-Switch and RFC5171 operation modes.

Values must be specified as multiples of 10 ms (7000 ms is allowed but 7005 ms is not a valid setting).

Switch mode can be configured to support under 100ms (HPE Aruba Networking 8325, 9300, or 10000 Switch series) unidirectional link detection times.

For example, for an HPE Aruba Networking 8325 switch to achieve 60ms failure detection times, interval can be set to 20ms and retries to 3.



---

Sessions under 100ms total detection time are susceptible to increasing processing load on the system. It is advisable to experiment with values that provide adequate detection times and system/protocol stability. HPE Aruba Networking recommends additional testing prior to configuring these sessions on a production environment.

---

However, these settings are recommended for specific deployments only, such as using UDLD for Ethernet Ring Protection Switching (ERPS) link-failure detection. The minimum detection time appropriate for your environment depends on the specific device family and configuration on which the protocol and system load is running. HPE Aruba Networking recommends additional testing for these configurations. During testing, monitor for unexpected false positive detections (i.e., UDLD records a failure when there was not any) on the interfaces running UDLD. Such false positive failures are an indication that the interval configuration requires tuning and that the system load might not allow such configuration.

The following table shows the fastest failure detection times that have been tested as a function of the UDLD enabled links. More UDLD links increase the processing load on the system and hence require higher interval values. Setting the interval to a lower value than recommended following might cause unexpected false positive detections. The values on this table are the unidimensional tested limits.

The values provided focus on the scalability of UDLD. The links column is the number of interfaces where UDLD is enabled given as a range. The interval column is the minimum interval value recommended for that scale. The detection time column is the total detection time that is achieved with those settings. For more than 16 links, the interval must be set to 200ms or higher.

| Links | Interval | v | Detection Time |
|-------|----------|---|----------------|
| 1-4   | 20ms     | 3 | 60ms           |
| 5-8   | 40ms     | 3 | 120ms          |
| 9-16  | 80ms     | 3 | 240ms          |
| 16+   | 200ms    | 3 | 600ms          |



---

When configuring detection times under 100ms for LAG interfaces, consider adding the interface first to the LAG and then enabling UDLD in the interface, to avoid false positive link failure detections. Adding an interface to a LAG causes momentary control plane traffic interruption for up to 100ms, which UDLD detects as a link failure if the detection time is following the control traffic interruption interval.

---

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| <TIME>    | Specifies the packet transmission interval. Range: 200 ms to 90000 ms (in increments of 10). |

## Examples

Setting the packet transmission interval to **1000** ms on interface **1/1/1**.

```
switch(config)# interface 1/1/1
switch(config-if)# udld interval 1000
```

Setting the packet transmission interval on interface **1/1/1** to the default value.

```
switch(config)# interface 1/1/1
switch(config-if)# no udld interval
```

Trying to set the packet interval to 1055 ms on interface 1 is rejected because the interval must be specified as a multiple of 10:

```
switch(config)# interface 1
switch(config-if)# udld interval 1055
Invalid interval. The interval value must be between 20ms and 90000ms and should be
specified as a multiple of 10, for example: 20, 100, 3000 or 90000.
```

Trying to set the packet interval to less than 7000 ms on interface 1 is rejected if using the RFC5171 mode.

```
switch(config)# interface 1
switch(config-if)# udld mode rfc5171 normal
switch(config-if)# udld interval 1000
Invalid interval. The interval must be equal or greater than 7000ms.
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

# udld mode

```
udld mode aruba-os {verify-then-forward | forward-then-verify}
udld mode rfc5171 <RFC5171-MODE>
no udld mode [[aruba-os [verify-then-forward | forward-then-verify]] | [rfc5171
[<RFC5171-MODE>]]]
```

## Description

Sets the operating mode.

The **no** form of this command sets the operating mode to the default value of **aruba-os** and **forward-then-verify**.

| Parameter                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>aruba-os {verify-then-forward   forward-then-verify}</code> | Selects the ArubaOS mode to use. Use this mode when interconnecting with HPE PVOS/Brocade/Foundry switches.                                                                                                                                                                                                                                                                                                                        |
| <code>verify-then-forward</code>                                  | In this mode: <ul style="list-style-type: none"><li>■ Interfaces start as unblocked.</li><li>■ Once an interface is determined to be bidirectional, it is blocked if the retry limit is reached without receiving any UDLD packets.</li><li>■ Interfaces automatically unblock if a UDLD packet is received.</li><li>■ On failover, the UDLD state does not change if the (interval * retries) time is around 6 seconds.</li></ul> |
| <code>forward-then-verify</code>                                  | In this mode: <ul style="list-style-type: none"><li>■ Interfaces start as unblocked.</li><li>■ Interfaces transition to the unblocked state when receiving UDLD packets.</li><li>■ Once an interface is determined to be bidirectional, it is blocked if the retry limit is reached without receiving any UDLD packets.</li><li>■ Interfaces automatically unblock if a UDLD packet is received.</li></ul>                         |
| <code>rfc5171 &lt;RFC5171-MODE&gt;</code>                         | Selects the RFC5171 mode to use. Use this mode when interconnecting with third-party switches.                                                                                                                                                                                                                                                                                                                                     |
| <code>normal</code>                                               | In this mode: <ul style="list-style-type: none"><li>■ Interfaces start as unblocked.</li><li>■ Interfaces do not block when the retry limit is reached without receiving any UDLD packets (plus 8 extra packets sent to the peer). Instead, an event is generated.</li><li>■ Interfaces automatically unblock if a UDLD packet is received.</li></ul>                                                                              |
| <code>aggressive</code>                                           | In this mode: <ul style="list-style-type: none"><li>■ Interfaces start as unblocked.</li><li>■ Once an interface is determined to be bidirectional, an interface will block when the retry limit is reached without receiving any UDLD packets (plus 8 extra packets sent to the peer).</li><li>■ Interfaces implement a limited/reduced errDisabled recovery</li></ul>                                                            |

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | mechanism. When the interface's state goes to errDisabled, a maximum of 3 attempts (5 minutes apart) are triggered to try and bring up the interface in case the remote endpoint is still sending UDLD packets. After these 3 retries, the interface will remain blocked even if UDLD packets are received. The only way to unblock the interface when this occurs is to disable (and optionally re-enable) UDLD on the interface. The retry limit is reset once the interface becomes unblocked. |

## Examples

Setting the operating mode to **aruba-os** and **forward-then-verify** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# udld mode aruba-os forward-then-verify
```

Setting the operating mode to **rfc5171** and **aggressive** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# udld mode rfc5171 aggressive
```

Setting the operating mode on interface **1/1/1** to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no udld mode
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## udld retries

```
udld retries <COUNT>
no udld retries [<COUNT>]
```

## Description

Sets the UDLD retry count.

The **no** form of this command sets the retry count to the default of 4.

| Parameter                  | Description                                                 |
|----------------------------|-------------------------------------------------------------|
| <code>&lt;COUNT&gt;</code> | Specifies the UDLD retry count. Range: 3 to 10. Default: 4. |

## Examples

Setting the UDLD retry count to **5** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# udld retries 5
```

Setting the UDLD retry count on interface **1/1/1** to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no udld retries
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## debug ufd all

debug ufd all  
no debug ufd all

### Description

Enables the UFD debug logs.  
The no form of this command disables the UFD debug logs.

### Examples

Enabling UFD debug logs:

```
switch(config)# debug ufd all
```

Disabling UFD debug logs:

```
switch(config)# no debug ufd all
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.09   | Command introduced. |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## delay

delay {down | up} <DELAY>  
no delay {down | up} <DELAY>

### Description

Within the selected UFD (Uplink Failure Detection) session context, specifies the amount of time (in seconds) to delay before bringing up or down the configured Links to Disable (LtD) after the corresponding Links to Monitor (LtM) come back up or go down.

For example, with **delay down 10**, when **all LtM links go down** and remain down after 10 seconds, UFD disables the interfaces/LAGs configured as Links-to-Disable (LtD). Similarly, with **delay up 10**, if **any of the LtM links come back up** and remain up after 10 seconds, then all the LtD links are brought back up.



In addition to any configured delay there is an additional delay of 3 to 5 seconds before bringing any Links-to-Disable (LtD) down or back up. So with the default delay of 0 seconds, a delay of 3 to 5 seconds does occur.

The no form of this command restores the delay to its default of 0 seconds.

| Parameter | Description                                                               |
|-----------|---------------------------------------------------------------------------|
| <DELAY>   | Species the delay in seconds. Range 0 to 180 seconds. Default: 0 seconds. |

## Examples

Setting the up and down delays to 10 seconds:

```
switch(config)# ufd enable
switch(config)# ufd session-id 1
switch(config-ufd-1)# links-to-monitor 1/1/1,1/1/2
switch(config-ufd-1)# links-to-disable 1/1/11,1/1/12
switch(config-ufd-1)# delay down 10
switch(config-ufd-1)# delay up 10
switch(config-ufd-1)# exit
switch(config)#
```

Resetting the up and down delays to their default of 0:

```
switch(config-ufd-1)# no delay down 10
switch(config-ufd-1)# no delay up 10
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.09   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-ufd-<ID> | Administrators or local user group members with execution rights for this command. |



# links-to-disable

```
links-to-disable <IF/LAG-LIST>
no links-to-disable <IF/LAG-LIST>
```

## Description

Within the selected UFD (Uplink Failure Detection) session context, specifies the interfaces or LAGs to disable when the monitored uplink interfaces go down.

For proper UFD operation, **links-to-disable** and **links-to-monitor** must both be configured. Use command **links-to-monitor** to specify a corresponding list of interfaces/LAGs to monitor.

The no form of this command deletes the specified links to disable list within the selected UFD session context.



---

A LAG member interface cannot be added as a link to disable. A interface configured as a link to disable cannot be added as a LAG member interface.

---

| Parameter                        | Description                                                                                                                                                   |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;IF/LAG-LIST&gt;</code> | List of L2 interfaces or LAGs. Separate interfaces/LAGs with commas (for individual interfaces/LAGs) or hyphens (for a consecutive range of interfaces/LAGs). |

## Examples

Configuring two links to be disabled:

```
switch(config)# ufd enable
switch(config)# ufd session-id 1
switch(config-ufd-1)# links-to-monitor 1/1/1,1/1/2
switch(config-ufd-1)# links-to-disable 1/1/11,1/1/12
switch(config-ufd-1)# delay down 10
switch(config-ufd-1)# delay up 10
switch(config-ufd-1)# exit
switch(config)#
```

Configuring a range of interfaces to disable:

```
switch(config)# ufd session-id 2
switch(config-ufd-2)# links-to-monitor lag18-lag20
switch(config-ufd-2)# links-to-disable 1/1/3-1/1/5
switch(config-ufd-2)# exit
switch(config)#
```

Deleting the links to disable for two interfaces:

```
switch(config-ufd-1)# no links-to-disable 1/1/11,1/1/12
```



---

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

---

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.09   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-ufd-<ID> | Administrators or local user group members with execution rights for this command. |

## links-to-monitor

```
links-to-monitor <IF/LAG-LIST>
no links-to-monitor <IF/LAG-LIST>
```

### Description

Within the selected UFD (Uplink Failure Detection) session context, specifies the uplink interfaces or LAGs to monitor for UFD.

For proper UFD operation, **links-to-monitor** and **links-to-disable** must both be configured. Use command **links-to-disable** to specify a corresponding list of interfaces/LAGs to disable if the monitored uplinks go down.

The no form of this command deletes the specified links to monitor list within the selected UFD session context.



A LAG member interface cannot be added as a link to monitor. A interface configured as a link to monitor cannot be added as a LAG member interface.

| Parameter     | Description                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IF/LAG-LIST> | List of L2 interfaces or LAGs. Separate interfaces/LAGs with commas (for individual interfaces/LAGs) or hyphens (for a consecutive range of interfaces/LAGs). |

### Examples

Configuring two uplinks to monitor for UFD session 1:

```
switch(config)# ufd enable
switch(config)# ufd session-id 1
switch(config-ufd-1)# links-to-monitor 1/1/1,1/1/2
switch(config-ufd-1)# links-to-disable 1/1/11,1/1/12
switch(config-ufd-1)# delay down 10
switch(config-ufd-1)# delay up 10
switch(config-ufd-1)# exit
switch(config)#
```

Configuring a range of uplink LAGs to monitor for UFD session 2:

```
switch(config)# ufd session-id 2
switch(config-ufd-2)# links-to-monitor lag18-lag20
switch(config-ufd-2)# links-to-disable 1/1/3-1/1/5
switch(config-ufd-2)# exit
switch(config)#
```

Deleting both links to monitor for UFD session 1:

```
switch(config-ufd-1)# no links-to-monitor 1/1/1,1/1/2
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.09   | Command introduced. |

## Command Information

| Platforms     | Command context               | Authority                                                                          |
|---------------|-------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-ufd- <i>&lt;ID&gt;</i> | Administrators or local user group members with execution rights for this command. |

## ufd enable

```
ufd enable
no ufd enable
```

### Description

Enables UFD (Uplink Failure Detection). UFD is disabled by default. This command must be issued before the configuration that is set with related UFD commands takes effect.

The no form of this command disables UFD.

### Examples

Enabling UFD:

```
switch(config)# ufd enable
switch(config)# ufd session-id 1
switch(config-ufd-1)# links-to-monitor 1/1/1,1/1/2
switch(config-ufd-1)# links-to-disable 1/1/11,1/1/12
switch(config-ufd-1)# delay down 10
switch(config-ufd-1)# delay up 10
switch(config-ufd-1)# exit
switch(config)#
```

Disabling UFD:

```
switch(config)# no ufd enable
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.09   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ufd session-id

```
ufd session-id <ID>
no ufd session-id <ID>
```

## Description

Creates the specified UFD (Uplink Failure Detection) session and then enters its context. If the specified session already exists, this command enters its context.

The no form of this command deletes the specified session configuration.

| Parameter | Description                                    |
|-----------|------------------------------------------------|
| <ID>      | Specifies the UFD session ID. Range: 1 to 128. |

## Examples

Creating UFD session 1 and then entering its context:

```
switch(config)# ufd enable
switch(config)# ufd session-id 1
switch(config-ufd-1)# links-to-monitor 1/1/1,1/1/2
switch(config-ufd-1)# links-to-disable 1/1/11,1/1/12
switch(config-ufd-1)# delay down 10
switch(config-ufd-1)# delay up 10
switch(config-ufd-1)# exit
switch(config)#
```

Creating UFD session 2 and then entering its context:

```
switch(config)# ufd session-id 2
switch(config-ufd-2)# links-to-monitor lag18-lag20
switch(config-ufd-2)# links-to-disable 1/1/3-1/1/5
switch(config-ufd-2)# exit
switch(config)#
```

Deleting UFD session 1:

```
switch(config)# no ufd session-id 1
```



For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.09   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

### ip forward-protocol udp

```
ip forward-protocol udp <IPv4-ADDR> {<PORT-NUM> | <PROTOCOL>}
no ip forward-protocol udp
```

#### Description

Defines the UDP server to which the interface forwards ingress UDP broadcast packets received on a specific UDP port. A maximum of 8 UDP broadcast servers can be configured per interface.

The **no** form of this command removes traffic forwarding for the specified server and port/protocol.

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv4-ADDR> | Specifies the UDP server IP address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <PORT-NUM>  | Specifies the UDP port number for which traffic is forwarded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <PROTOCOL>  | Specifies the protocol name for which traffic is forwarded. Supported protocols and their port numbers are: <ul style="list-style-type: none"><li>■ dns (53): Domain Name Service</li><li>■ ntp (123): Network Time Protocol</li><li>■ netbios-ns (137): NetBIOS Name Service</li><li>■ netbios-dgm (138): NetBIOS Datagram Service</li><li>■ radius (1812): Remote Authentication Dial-In User Service</li><li>■ radius-old (1645): Remote Authentication Dial-In User Service</li><li>■ rip (520): Routing Information Protocol</li><li>■ snmp (161): Simple Network Management Protocol</li><li>■ snmp-trap (162): Simple Network Management Protocol</li><li>■ tftp (69): Trivial File Transfer Protocol</li><li>■ timep (37): Time Protocol</li></ul> |

#### Examples

*On the 6400 Switch Series, interface identification differs.*

Forwarding DNS traffic to server 192.168.1.10 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip udp-bcast-forward protocol udp 192.168.1.10 dns
```

Forwarding DNS traffic (port 53) to server 192.168.1.10 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip udp-bcast-forward protocol udp 192.168.1.10 53
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

# ip udp-bcast-forward

```
ip udp-bcast-forward
no ip udp-bcast-forward
```

## Description

Enables UDP broadcast forwarding.

The **no** form of this command disables UDP broadcast forwarding.

## Examples

Enabling UDP broadcast forwarding:

```
switch(config)# ip udp-bcast-forward
```

Disabling UDP broadcast forwarding:

```
switch(config)# no ip udp-bcast-forward
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# show ip forward-protocol udp

```
show ip forward-protocol udp [<INTERFACE-NAME>] [vsx-peer]
```

## Description

Shows the configured UDP forwarding settings for all interfaces or a specific interface.

| Parameter        | Description                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-NAME> | Specifies the name of an interface. Format: member/slot/port.                                                                                                                                                                    |
| [vsx-peer]       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Showing the configured UDP forwarding settings for all interfaces:

```
switch# show ip forward-protocol udp
UDP Broadcast Forwarder : enabled

Interface: 1/1/1
IP Forward Address UDP Port

2.2.2.2 1645
4.4.4.4 138
4.4.4.4 1812
1.1.1.1 53
8.1.1.1 123
8.1.1.1 137
Interface: 1/1/2
IP Forward Address UDP Port

2.2.2.2 37
2.2.2.2 69
2.2.2.2 520
2.2.2.2 161
2.2.2.2 162
```

Showing the configured UDP forwarding settings for a specific interface:

```
switch# show ip forward-protocol udp interface 1/1/1
UDP Broadcast Forwarder : enabled

Interface: 1/1/1
IP Forward Address UDP Port

2.2.2.2 1645
4.4.4.4 138
4.4.4.4 1812
1.1.1.1 53
8.1.1.1 123
8.1.1.1 137
```

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |



## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## password complexity

```
password complexity
no password complexity
```

### Description

Enters the password-complexity context (shown in the switch prompt as **config-pwd-cplx**) for the purpose of enabling and configuring password complexity. Password complexity enhances security by enforcing specific password complexity requirements. Password complexity is disabled by default and must be enabled by execution of the **enable** command.

Enabling or changing password complexity settings effects password creation or password change after the password complexity feature is enabled or changed. All existing passwords will continue to function as currently configured. When existing passwords are changed they will have to comply with whatever password complexity settings are enabled at the time of the change.

The **no** form of this command reverts all settings to their default values and disables password complexity enforcement.



To ensure that enhanced security is maintained, it is recommended that you do not set any values to less than their defaults.



Password complexity applies only to local authentication. For remote authentication, you may choose to set up an equivalent of password complexity according to whatever is supported on your particular TACACS+ or RADIUS server.

### Subcommands

These subcommands are available within the password complexity context (shown in the switch prompt as **config-pwd-cplx**).

**enable**

Enables password complexity enforcement. The enforcement only applies to passwords created after this enabling. Existing passwords are not checked against password complexity.

**disable**

Disables password complexity enforcement.

**[no] history-count <COUNT>**

Specifies the number of previous passwords checked to prevent excessive reuse. Not applicable when adding new users. The **no** form of this subcommand resets the value to its default. Default: 5. Range: 1 to 5.



Previous passwords checked includes passwords used prior to enabling the password complexity feature.

**[no] minimum-length <LENGTH>**

Specifies the minimum password length. The no form of this subcommand resets the value to its default. Default: 8. Range: 1 to 32.

[no] position-changes <POSITIONS>

Specifies the minimum number of characters that must change in the new password compared to the previous password. Not applicable if no previous password exists, including when adding new users. The no form of this subcommand resets the value to its default. Default: 8. Range: 1 to 32.

The number of password position changes is based on the number of simple character insertions, deletions, or replacements. For example:

Old password: abCD4\$ New password: abCD\$ Position changes=1 ("4" deleted) Old password: abCD4\$ New password: abCDEF4\$ Position changes=2 ("EF" inserted) Old password: abCD4\$ New password: ebCD4\$ Position changes=2 ("a" replaced with "e," "1" added) Old password: abCD4\$ New password: abC\$# Position changes=3 ("D4" deleted, "#" added)

[no] lowercase-count <COUNT>

Specifies the minimum lowercase character count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] uppercase-count <COUNT>

Specifies the minimum uppercase character count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] numeric-count <COUNT>

Specifies the minimum numeric digit count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] special-char-count <COUNT>

Specifies the minimum special character count for new passwords. The no form of this subcommand resets the value to its default. Default: 1. Range: 0 to 32.

[no] adjacent-char-type-count

Specifies the maximum number of adjacent characters from a character set allowed in a password. The different character sets are:

- Numbers
- Lowercase alphabets
- Uppercase alphabets
- Special characters

The number of adjacent characters from the character set in the password has to be less than or equal to the configured value. When set to 0, adjacent character type length check requirement is disabled. The no form of this subcommand resets the value to its default. Default: 0. Range: 0-31.

list

List the subcommands available within the password complexity context.

exit

Exits the password complexity context.

end

Exits the password complexity context and then the config context.

## Usage

- Password complexity is only for use with plaintext passwords. With password complexity enabled, existing ciphertext passwords will continue working until a password is changed. All new passwords must be entered in plaintext form and be compliant with your password complexity configuration.
- The effective minimum password length may be larger than the configured **minimum-length** value. The effective minimum password length is calculated as follows:

LARGEST-of: (minimum-length, position-changes, (SUM-of: lowercase-count+uppercase-count+numeric-count+special-char-count))

For example, with **minimum-length=8**, and **position-changes=10** (and the sum of the other four count settings **<=9**), the **effective minimum-length is 10** (because **position-changes** is largest). Similarly, with a **minimum-length=12**, **position-changes=8**, **lowercase-count=8**, **uppercase-count=4**, **numeric-count=1**, **special-char-count=1**, the **effective minimum-length is 14** ( $8+4+1+1=14$ ) (because sum of the four counts is largest).

## Examples

Configuring password complexity settings with an effective minimum length of 10 (because **position-changes** is 10):

```
switch(config)# password complexity
switch(config-pwd-cplx)# history-count 3
switch(config-pwd-cplx)# minimum-length 8
switch(config-pwd-cplx)# position-changes 10
switch(config-pwd-cplx)# lowercase-count 2
switch(config-pwd-cplx)# uppercase-count 2
switch(config-pwd-cplx)# numeric-count 2
switch(config-pwd-cplx)# special-char-count 2
switch(config-pwd-cplx)# adjacent-char-type-count 3
switch(config-pwd-cplx)# enable
switch# exit
```

Configuring password complexity settings with an effective minimum length of 14 (because the sum of the four count items is 14):

```
switch(config)# password complexity
switch(config-pwd-cplx)# history-count 4
switch(config-pwd-cplx)# minimum-length 12
switch(config-pwd-cplx)# position-changes 8
switch(config-pwd-cplx)# lowercase-count 8
switch(config-pwd-cplx)# uppercase-count 4
switch(config-pwd-cplx)# numeric-count 1
switch(config-pwd-cplx)# special-char-count 1
switch(config-pwd-cplx)# adjacent-char-type-count 3
switch(config-pwd-cplx)# enable
switch# exit
```

Enabling password complexity (with default settings) and changing a user (admin1) password successfully but failing to change another user (admin2) password due to not meeting complexity requirements:

```
switch(config)# password complexity
switch(config-pwd-cplx)# enable
switch(config-pwd-cplx)# exit
switch(config)#
switch(config)# user admin1 password
Changing password for user admin1
Enter old password:*****
Enter new password:*****
Confirm new password:*****
switch(config)#
switch(config)# user admin2 password
Changing password for user admin2
Enter old password:*****
Enter new password:*****
Confirm new password:*****
```

```

User password not changed.
The new password does not meet one or more of the following complexity
requirements:
Minimum length : 8
Position changes : 8
Numeric count : 1
Lowercase count : 1
Uppercase count : 1
Special character count : 1
Adjacent character type count: 3

```

With password complexity already enabled, attempting to change an existing user password but failing because the new password is identical to a recently used one (**history-count**).

```

switch(config)# user admin1 password
Changing password for user admin1
Enter old password:*****
Enter new password:*****
Confirm new password:*****
User password not changed.
The new password is the same as a recently used password.

```

With password complexity already enabled, creating a new admin user (admin3) with a plaintext password that meets complexity requirements.

```

switch(config)# user admin3 group administrators password
Adding user admin3
Enter password:*****
Confirm password:*****

```

With password complexity already enabled, attempting to create a new admin user (admin4) with a ciphertext password but failing because ciphertext passwords are not supported with password complexity enabled.

```

switch(config)# user admin4 group administrators password ciphertext AQBapPd...==
Ciphertext passwords cannot be used when password complexity is enabled.
switch(config)#

```

## Command History

| Release          | Modification                                      |
|------------------|---------------------------------------------------|
| 10.11.1010       | <b>adjacent-char-type-count</b> subcommand added. |
| 10.07 or earlier | --                                                |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# user

```
user <USERNAME> group {administrators | operators | auditors | <USER-GROUP>}
 password [ciphertext <CIPHERTEXT-PASSWORD> | plaintext <PLAINTEXT-PASSWORD>]
no user <USERNAME>
```

## Description

Creates a user and adds the user to one of the user groups. Users are given the privileges of their group. For the three built-in user groups (administrators, operators, auditors), the privileges are fixed. For user-defined local user groups, the privileges are defined by the CLI command authorization rules of the group.

When entered without either optional ciphertext or plaintext parameters, the cleartext password is prompted for twice, with the characters entered masked with "\*" symbols.



Built-in users including admin cannot be deleted. The user account of the current session cannot be deleted. When a user account is deleted, all of that user's active SSH sessions are terminated.

The **no** form of this command removes a user account from the switch. The administrator cannot delete the user account from which they are logged in. The **admin** user cannot be deleted.

| Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <USERNAME>                            | <p>Specifies the user name. Requirements:</p> <ul style="list-style-type: none"><li>Must start with a lowercase or uppercase letter.</li><li>Can contain numbers, lowercase, and uppercase letters.</li><li>Can include only these three special characters: hyphens ( - ), dots ( . ), and underscores ( _ ).</li><li>Can have a maximum of 32 characters.</li><li>Cannot be empty.</li><li>Cannot be: admin, root, or remote_user.</li><li>Cannot be Linux reserved names such as:<br/>daemon, bin, sys, sync, proxy, www-data, backup, list, irc, gnats, nobody, systemd-bus-proxy, sshd, messagebus, rpc, systemd-journal-gateway, systemd-journal-remote, systemd-journal-upload, systemd-timesync, systemd-coredump, systemd-resolve, rpcuser, vagrant, opsd, rdanet, _lldpd, rdaadmin, rdaweb, docker_container, tss.</li></ul> <p><b>NOTE:</b> Usernames containing the same consecutive letters with varying capitalization, such as Admin, ADMIN, and aDmin, will each be treated as different customer-configured user accounts.</p> |
| group                                 | Selects the local user group to which the new user will be assigned.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| administrators   operators   auditors | Selects one of three built-in local user groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <USER-GROUP>                          | Specifies an existing user-defined local user group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ciphertext <CIPHERTEXT-PASSWORD>      | Specifies a ciphertext password. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. The variable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Parameter                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | <p><code>&lt;CIPHERTEXT-PASSWORD&gt;</code> is Base64 and is typically copied from another switch using the <code>show running-config</code> command output and then pasted into this command.</p> <p><b>NOTE:</b> The administrator cannot construct ciphertext passwords themselves. The ciphertext is only created by an AOS-CX switch. The ciphertext is created by setting a password for a user with the <code>user</code> command. The ciphertext is available for copying from the <code>show running-config</code> output and pasting into the configuration on any other AOS-CX switch. The target switch must have the same export password (default or otherwise) as the source switch.</p> |
| <code>plaintext &lt;PLAINTEXT-PASSWORD&gt;</code> | Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Usage

- Up to 63 local users can be added, for a total of 64 users including the default user **admin**. A user can belong to only one group.
- The switch ships with the **admin** user account and three built-in local user groups: **administrators**, **operators**, and **auditors**. The **admin** account belongs to the **administrators** group. The Service OS also includes the administrator user **admin**. The two admin users are entirely distinct.
- When a local user account is removed, the user loses all active login/SSH sessions. Any calls on the existing REST session with that local user account fail with a permissions issue as soon as the user is deleted. Soon afterwards, the existing REST sessions with the deleted local user account become invalidated. If a user is viewing the GUI while their account is deleted, the user is redirected to the login page within 60 seconds. The home directory associated with the user is also removed from the switch.
- Cleartext passwords (whether entered with prompting or entered directly) must:
  - Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [`\x21-\x7E`] (decimal 33 to 126). Spaces are not allowed. When the password is entered directly without prompting, the "?" symbol (hexadecimal 3F [`\x3F`] (decimal 63)) is not permitted.
  - Contain at most 32 characters.
  - Contain at least the number of characters configured (optionally) for `minimum-password-length`.



Although empty passwords are supported, it is recommended that you use strong passwords for all production switches.



---

Only an administrator can change the password of a user assigned to the `operators` role.

---

Although usernames with uppercase letters appear in the show-running configuration, users will not have login access if the username was configured and downgraded to a version without uppercase support.

---

## Examples

Creating local user **jamie** in the **administrators** group with a prompted password:

```
switch(config)# user jamie group administrators password
Adding user jamie
Enter password:*****
Confirm password:*****
```

Creating user **chris** in the existing user-defined local user group **admuser2** with a cleartext password, using direct entry without prompting:

```
switch(config)# user chris group admuser2 password plaintext passWORDxJ|989
```

Creating user **alex** in the **operators** group with a ciphertext password (the ciphertext shown is a placeholder that must be replaced with actual ciphertext):

```
switch(config)# user alex group operators password ciphertext NDcDI2...8igJfA=
```

Removing user **jamie**:

```
switch(config)# no user jamie
User jamie's home directory and active sessions will be deleted.
Do you want to continue [y/n]?y
```

Using uppercase letters within username:

```
switch(config)# user TestUser1 group administrators password plaintext testuser1
switch(config)#
```



---

For more information on features that use this command, refer to the Multicast Guide for your switch model.

---

## Command History

| Release          | Modification                                                |
|------------------|-------------------------------------------------------------|
| 10.13            | Added support for use of uppercase letters within username. |
| 10.07 or earlier | --                                                          |

## Command Information



| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## user enable

```
user <USERNAME> enable
no user <USERNAME> disable
```

### Description

Re-enables a disabled user. When a user account is re-enabled, the most recently configured password and all configured authorized keys will be restored.

| Parameter  | Description       |
|------------|-------------------|
| <USERNAME> | Name of the user. |

### Examples

Re-enabling user **admin**:

```
switch(config)# user admin enable
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

### Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## user disable

```
user <USERNAME> disable
no user <USERNAME> enable
```

### Description

Disables the specified user name. Only the built-in "admin" user can be disabled. No other users can be disabled. Non built-in users should be deleted instead. There must always be at least one enabled administrator account. The user account of the current session cannot be disabled. This rule has an implication on config download and restore. If a local admin user applies a checkpoint or external config

in JSON format the user will be disabled and the sessions will close. If a local admin user applies an external config in CLI format then the "user admin disable" directive will not be applied, an error will be returned, and a log entry will be made. The local admin user's sessions will not be closed since the directive was not applied. To disable the admin user the user must first log out, then log back in as another admin user and execute the "user admin disable" directive.

When a user account is disabled, all of that user's active SSH sessions are terminated. A user's password and authorized-keys can be changed during disablement, however the user will remain disabled.

After a user is disabled all use of that user should fail whether explicitly or implicitly. For example, Central on-boarding using the built-in admin account will fail if admin is disabled.

Only the built-in "admin" user can be disabled. No other users can be disabled. It has no impact on users configured on remote authentication servers. For example, after local admin is disabled, a user can still log in as admin via RADIUS authentication if admin is configured as a user on RADIUS server.

| Parameter  | Description       |
|------------|-------------------|
| <USERNAME> | Name of the user. |

## Examples

Disabling the user **admin**:

```
switch(config)# user admin disable
All active sessions for user admin will be closed.
Continue (y/n)? y
```



For more information on features that use this command, refer to the Multicast Guide for your switch model.

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.17   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## user-group

```
user-group <GROUP-NAME>
no user-group <GROUP-NAME>
```

## Description

If <GROUP-NAME> does not exist, this command creates a local user group and then enters its context. If <GROUP-NAME> exists, this command enters the context for the specified <GROUP-NAME>. Within

the **<GROUP-NAME>** context, several subcommands are available for working with rules that specify what CLI commands are permitted or denied for all members of the local group.

In addition to the three built-in user groups **administrators**, **operators**, and **auditors**, up to 29 user-defined local user groups can be defined. All users can be members of only one of the up to 32 groups. The **no** form of this command deletes the specified user group. All members of the deleted group lose all command authorization privilege.

| Parameter                       | Description                                                                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;GROUP-NAME&gt;</code> | Specify a user group name up to 32 characters long. A new group is created if the specified group does not exist and then the group context is entered. If the group name exists, its context is entered. |



Do not causally delete user-defined local user groups without understanding the implications. Although user-defined local user groups can be deleted with the respective members losing all privileges, the three built-in groups `administrators`, `operators`, and `auditors` are always available and their privileges are unchangeable.

## Subcommands

These subcommands are available within the user-defined local user group context (shown in the switch prompt as **config-usr-grp-<GROUP-NAME>**).

```
[<SEQ-NUM>] {permit | deny} cli command "<REGEX>"
no <SEQ-NUM>
```

Defines a CLI command privilege **permit** or **deny** rule. There is an implicit **"deny .\*"** rule at the end of every user-defined group rule list. Members of a user-defined group without any **permit** rules have no CLI command privileges.

The **no** form of this subcommand deletes the specified (by sequence number) rule from the group.



Rule evaluation proceeds from lowest to highest sequence number until the first successful match, resulting in either CLI command permission or denial. Rule evaluation ceases upon first match. Therefore, rules for related CLI commands must be defined in most restrictive to least restrictive order.

`<SEQ-NUM>`

Specifies the CLI command rule sequence number. When omitted, a sequence number that is 10 greater the highest existing sequence number is auto-assigned. When no rules exist, the first auto-assigned sequence number is 10.

`{permit | deny}`

Sets the rule type as either **permit** or **deny**. Rule order is important. For example, these two related rules together authorize all **show** commands except for the **show aaa** commands.

```
switch(config-usr-grp-admuser2)#10 deny cli command "show aaa .*"
switch(config-usr-grp-admuser2)#20 permit cli command "show .*"

```

To achieve the wanted effect in this example, the **deny** rule must precede the **permit** rule. These two rules together achieve the following:

- All **show aaa** commands match on rule 10, triggering command denial, and the immediate cessation of further rule evaluation. Matching on rule 20 is never attempted.
- All other **show** commands (excluding **show aaa** commands) match on rule 20 and are therefore permitted.

#### <REGEX>

Specifies the CLI command matching criteria of the rule. The criteria can be expressed as **".\*"** which matches all commands. Otherwise, the criteria is expressed as a POSIX-compliant regular expression (regex) string starting with an exact match command token (for example **show**) followed by a regex representing command arguments. The first word must be a string that contains only alphanumeric or hyphen characters.

For example, to allow all commands starting with the word **interface**, the regex must be **"interface .\*"** or just **"interface"**. Using **"interface.\*"** (without the space) is not supported. For example, **"show .\*"** matches every **show** command. Consult the Extended regular expression information available at: [https://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1\\_chap09.html#tag\\_09\\_04](https://pubs.opengroup.org/onlinepubs/9699919799/basedefs/V1_chap09.html#tag_09_04).

| Sample matching criteria | Sample matched CLI command or specifier | Matches                            |
|--------------------------|-----------------------------------------|------------------------------------|
| show .*                  | show accounting log                     | All <b>show</b> commands           |
| bgp .*                   | bgp router-id 1.1.1.1                   | All <b>bgp</b> commands            |
| interface .*             | interface 1/1/1                         | All interface specifiers           |
| vlan (3 4)               | vlan 3                                  | VLAN 3 or 4                        |
| vlan [1-9]               | vlan 5                                  | A single VLAN in the range 1 to 9  |
| vlan ([1-9] 1[0-9])      | vlan 19                                 | A single VLAN in the range 1 to 19 |

[<SEQ-NUM>] comment <TEXT-STRING>

no <SEQ-NUM> comment

Adds a comment to an existing rule. The no form of this subcommand removes an existing comment.

```
switch(config-usr-grp-admuser2)# 10 comment Deny all show aaa commands.
switch(config-usr-grp-admuser2)# 20 comment Permit all other show commands.
switch(config-usr-grp-admuser2)#
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
 10 comment Deny all show aaa commands.
 10 deny cli command "show aaa .*"
 20 comment Permit all other show commands.
 20 permit cli command "show ."
```

include <GROUP-NAME> [no] include <GROUP-NAME>

Include all rules from the specified user-defined <GROUP-NAME>. Only one group can be included in the definition of another group. The content of the included group is effectively placed at the top of the rules list in the current group. If the specified <GROUP-NAME> does not exist, it is created.

The no form of this subcommand removes the specified included group from the current group. The specified included group must exist and must be included in the current group or else an error message is shown.

The name of the included group is shown at the top of the **show user-group** command for the group with the **include**.

In this example, group **admuser1** is included in group **admuser2**. So the **admuser1** rules are evaluated first and then the rules in the **admuser2** group are only evaluated if no CLI command match occurs for the rules in group **admuser1**.

```
switch(config-usr-grp-admuser2)# include admuser1
switch(config-usr-grp-admuser2)# show user-group admuser2
User Group Summary
=====
Name : admuser2
Type : configuration
Included Group : admuser1
Number of Rules : 2
User Group Rules
=====
SEQUENCE NUM ACTION COMMAND COMMENT

10 deny show aaa .* Deny all show aaa commands.
20 permit show .* Permit all other show
commands.
```

**resequence** [**<STARTING-SEQ-NUM>** **<INCREMENT>**]

Resequences the CLI command authorization rules. When entered without the optional parameters the rules are resequenced with a **<STARTING-SEQ-NUM>** of 10 and an **<INCREMENT>** of 10.

**<STARTING-SEQ-NUM>**

Specifies the starting sequence number.

**<INCREMENT>**

Specifies the sequence number increment.

Resequencing the rules to start at 100 with an increment of 20:

```
switch(config-usr-grp-admuser2)# resequence 100 20
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
 100 comment Deny all show aaa commands.
 100 deny cli command "show aaa .*"
 120 comment Permit all other show commands.
 120 permit cli command "show .*"
```

Resequencing the rules to the default of starting at 10 with an increment of 10:

```
switch(config-usr-grp-admuser2)# resequence
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
 10 comment Deny all show aaa commands.
 10 deny cli command "show aaa .*"
 20 comment Permit all other show commands.
 20 permit cli command "show .*"
```

**show running-config current-context**

Shows all the commands used to configure the rules in the current group context.

```
switch(config-usr-grp-admuser2)# show running-config current-context
user-group admuser2
 10 comment Deny all show aaa commands.
 10 deny cli command "show aaa .*"
 20 comment Permit all other show commands.
 20 permit cli command "show .*"

```

#### list

List the subcommands available within the user-defined group context.

#### exit

Exits the user-defined group context.

#### end

Exits the user-defined group context and then the config context.



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## user management-interface

```
user <USERNAME> management-interface <MGMT-INTERFACE>
no user <USERNAME> management-interface <MGMT-INTERFACE>

```

### Description

Enables a management interface for the specified local user. By default, all management interfaces are enabled for all local users.

The **no** form of this command disables the selected management interface for the specified local user.

| Parameter        | Description                                                                                                                                                                     |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <USERNAME>       | Specifies the name of an existing local user.                                                                                                                                   |
| <MGMT-INTERFACE> | Selects one of the management interfaces: <b>ssh</b> , <b>telnet</b> , <b>https-server</b> , <b>console</b> . Note that <b>https-server</b> corresponds to the Web UI and REST. |

### Examples

Enabling the SSH management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface ssh
```

Disabling the SSH management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface ssh
```

Enabling the telnet management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface telnet
```

Disabling the telnet management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface telnet
```

Enabling the https-server (Web UI) management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface https-server
```

Disabling the https-server (Web UI) management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface https-server
```

Enabling the console management interface for local user **admin1**:

```
switch(config)# user admin1 management-interface console
```

Disabling the console management interface for local user **admin1**:

```
switch(config)# no user admin1 management-interface console
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.11   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# user password

```
user <USERNAME> password [ciphertext <CIPHERTEXT-PASSWORD> | plaintext <PLAINTEXT-PASSWORD>]
```

## Description

Changes a password for an account or enables the password for the admin account. When entered without either optional **ciphertext** or **plaintext** parameters, the cleartext password is prompted for twice, with the characters entered masked with "\*" symbols.

| Parameter                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <USERNAME>                       | Specifies the corresponding user name for the password you want to change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ciphertext <CIPHERTEXT-PASSWORD> | <p>Specifies a ciphertext password. No password prompts are provided and the ciphertext password is validated before the configuration is applied for the user. The variable &lt;CIPHERTEXT-PASSWORD&gt; is Base64 and is typically copied from another switch using the <code>show running-config</code> command output and then pasted into this command.</p> <p><b>NOTE:</b> The administrator cannot construct ciphertext passwords themselves. The ciphertext is only created by an AOS-CX switch. The ciphertext is created by setting a password for a user with the <code>user</code> command. The ciphertext is available for copying from the <code>show running-config</code> output and pasting into the configuration on any other AOS-CX switch. The target switch must have the same export password (default or otherwise) as the source switch.</p> |
| plaintext <PLAINTEXT-PASSWORD>   | Specifies the password without prompting. The password is visible as cleartext when entered but is encrypted thereafter. Command history does show the password as cleartext.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Usage

The admin account is available on the switch without a password by default.

Cleartext passwords (whether entered with prompting or entered directly) must:

- Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [\x21-\x7E] (decimal 33 to 126). Spaces are not allowed. When the password is entered directly without prompting, the "?" symbol (hexadecimal 3F [\x3F] (decimal 63)) is not permitted.
- Contain at most 32 characters.
- Contain at least the number of characters configured (optionally) for `minimum-password-length`.



Although empty passwords are supported, it is recommended that you use strong passwords for all production switches.





---

Only an administrator can change the password of a user assigned to the `operators` role.

---

Although usernames with uppercase letters appear in the show-running configuration, users will not have login access if the username was configured and downgraded to a version without uppercase support.

---

## Examples

Enabling (or changing) a cleartext password for **admin**:

```
switch(config)# user admin password
Changing password for user admin
Enter password:*****
Confirm password:*****
```

Changing the cleartext password for user **chris**, using direct entry without prompting:

```
switch(config)# user chris password plaintext PASSwordZQ#@67
```

Changing the ciphertext password for user **alex** (the ciphertext shown is a placeholder that must be replaced with actual ciphertext):

```
switch(config)# user alex password ciphertext XqYJ36...W83D4Y=
```



---

For more information on features that use this command, refer to the Security Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## service export-password

```
service export-password
no service export-password
```

## Description

Configures a nondefault export password. The export password is used to transform critical security parameters (such as password hashes) into ciphertext suitable for exporting and showing by

commands such as **show running-config**. This transformation enables safe switch configuration import and export.

The **no** form of this command reverts the export password to its factory default.



---

All factory-default switches have identical default export passwords. For security, it is recommended that you set the same nondefault export password on every switch in a group that will exchange configuration information. Only switches with identical export passwords can exchange configuration information.

---

## Usage

Prompts you twice for the new export password.

The export password must:

- Contain only ASCII characters from hexadecimal 21 to hexadecimal 7E [\x21-\x7E] (decimal 33 to 126). Spaces are not allowed.
- Contain at most 32 characters.
- Not be blank.

## Examples

Configuring a new export password:

```
switch(config)# service export-password
Enter password:*****
Confirm password:*****
```

Reverting the export password to its factory default:

```
switch(config)# no service export-password
```



---

For more information on features that use this command, refer to the Security Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

# show password-complexity

show password-complexity

## Description

Shows user-configured or default password complexity checking criteria.

## Examples

Showing the current password complexity checking criteria:

```
switch(config)# show password-complexity

Global password complexity checking criteria:
 Password complexity : Enabled
 Previous passwords to check : 3
 Minimum password length : 12
 Minimum position changes : 10
 Maximum adjacent characters count : 3
 Password composition
 Minimum lowercase characters : 3
 Minimum uppercase characters : 1
 Minimum special characters : 1
 Minimum numeric characters : 3
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show user-group

`show user-group [<GROUP-NAME>] [vsx-peer]`

### Description

Shows user group information for the built-in groups plus any user-defined local user groups. When entered without **<GROUP-NAME>**, summary information is shown for all groups.

| Parameter                 | Description                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;GROUP-NAME&gt;</b> | Narrows the <b>show</b> command output to that of the specified group, and for local user groups, adds the <b>User Group Rules</b> list.                                                                                         |
| <b>vsx-peer</b>           | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Show the list of all user groups, including built-in groups and local user groups.

```
switch# show user-group
GROUP NAME GROUP TYPE INCLUDED GROUP NUMBER OF RULES

administrators built-in n/a n/a
admuser1 configuration -- 5
admuser2 configuration admuser1 2
auditors built-in n/a n/a
operators built-in n/a n/a
```

Show detailed information for local user group **admuser2**.

```
switch(config-usr-grp-admuser2)# show user-group admuser2
User Group Summary
=====
Name : admuser2
Type : configuration
Included Group : admuser1
Number of Rules : 2
User Group Rules
=====
SEQUENCE NUM ACTION COMMAND COMMENT

10 deny show aaa .* Deny all show aaa commands.
20 permit show .* Permit all other show
commands.
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show user information

show user information

### Description

Shows the following information for the logged-in user:

- User name.
- User authentication type: **local**, **RADIUS**, or **TACACS+**.
- User group: **administrators**, **operators**, or **<GROUP-NAME>**. This field is not applicable for remote authenticated users who are mapped to administrators or operators based on their privilege level.
- User privilege level: For the built-in user groups and RADIUS or TACACS+, the role privilege level value is shown. For user-defined user groups, **N/A** is shown.
- User login session: **ssh**, **telnet**, **https-server**, or **console**.

## Examples

Showing information for the **admin** user:

```
switch# show user information
Username : admin
Authentication type : Local
User group : administrators
User privilege level : 15
User login session : console
```

Showing information for a member of the user-defined local user group **admuser2**:

```
switch# show user information
Username : admin2-b
Authentication type : Local
User group : admuser2
User privilege level : N/A
User login session : telnet
```

Showing information for a member of **operators**:

```
switch# show user information
Username : operator
Authentication type : Local
User group : operators
User privilege level : 1
User login session : https-server
```

Showing information for remote RADIUS user **rad\_user1** mapped to local user group **administrators**:

```
switch# show user information
Username : rad_user1
Authentication type : RADIUS
User group : administrators
User privilege level : 15
User login session : telnet
```

Showing information for remote RADIUS user **rad\_user2** mapped to local user group **operators**:

```
switch# show user information
Username : rad_user2
Authentication type : RADIUS
User group : operators
```

```
User privilege level : 1
User login session : console
```

Showing information for remote TACACS+ **tac\_user1** logged in with **priv-lvl** 15 (mapped to user group **administrators**):

```
switch# show user information
Username : tac_user1
Authentication type : TACACS+
User group : administrators
User privilege level : 15
User login session : ssh
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release          | Modification                                                             |
|------------------|--------------------------------------------------------------------------|
| 10.11            | Command now includes <b>User login session</b> information in its output |
| 10.07 or earlier | --                                                                       |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show user-list

```
show user-list [vsx-peer]
```

### Description

Shows all configured users and their corresponding group names.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Showing the list of configured users and their group names:

```
switch# show user-list
```

| User      | Group          | Status  |
|-----------|----------------|---------|
| admin     | administrators | enabled |
| ADMIN     | administrators | enabled |
| test1     | operators      | enabled |
| test2     | auditors       | enabled |
| Test2     | auditors       | enabled |
| TestUser1 | operators      | enabled |

Showing the list of configured users and their group names after disabling the user **admin**:

```
switch# show user-list
```

| User      | Group          | Status   |
|-----------|----------------|----------|
| admin     | administrators | disabled |
| ADMIN     | administrators | enabled  |
| test1     | operators      | enabled  |
| test2     | auditors       | enabled  |
| Test2     | auditors       | enabled  |
| TestUser1 | operators      | enabled  |



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release          | Modification        |
|------------------|---------------------|
| 10.17 or earlier | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show user-list management-interface

```
show user-list management-interface [vsx-peer]
```

### Description

Shows a list of local users and the enabled management interfaces for each user.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Disabling SSH and https-server for user **admin1**, disabling Telnet for **admin2**, then showing the configuration:

```
switch(config)# no user admin1 management-interface ssh
switch(config)# no user admin1 management-interface https-server
switch(config)# no user admin2 management-interface telnet
switch(config)# show user-list management-interface
USER ENABLED MANAGEMENT INTERFACE(S)

admin ssh,telnet,https-server,console
admin1 telnet,console
admin2 ssh, https-server, console
```

Re-enabling https-server for user **admin1**, re-enabling Telnet for **admin2**, then showing the configuration:

```
switch(config)# user admin1 management-interface https-server
switch(config)# user admin2 management-interface telnet
switch(config)# show user-list management-interface
USER ENABLED MANAGEMENT INTERFACE(S)

admin ssh,telnet,https-server,console
admin1 telnet,https-server,console
admin2 telnet,https-server,console
```



For more information on features that use this command, refer to the Security Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.11   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |



## description

description <DESCRIPTION>

### Description

Specifies a descriptive for a VLAN.

| Parameter     | Description                           |
|---------------|---------------------------------------|
| <DESCRIPTION> | Specifies a description for the VLAN. |

### Examples

Assigning a description to VLAN 20:

```
switch(config)# vlan 20
switch(config-vlan-20)# description primary
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context       | Authority                                                                          |
|---------------|-----------------------|------------------------------------------------------------------------------------|
| All platforms | config-vlan-<VLAN-ID> | Administrators or local user group members with execution rights for this command. |

## vlan name

name <VLAN-NAME>

### Description

Associates a name with a VLAN.

| Parameter   | Description                                                                                                    |
|-------------|----------------------------------------------------------------------------------------------------------------|
| <VLAN-NAME> | Specifies a name for a VLAN. Length: 1 to 32 alphanumeric characters, including underscore (_) and hyphen (-). |

## Usage

- Each named VLAN must have a unique name; there cannot be duplicate names for VLANs.
- By default, VLANs are created with the default name: VLAN <VLAN-ID>

## Examples

Assigning the name **backup** to VLAN 20:

```
switch(config)# vlan 20
switch(config-vlan-20)# name backup
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context       | Authority                                                                          |
|---------------|-----------------------|------------------------------------------------------------------------------------|
| All platforms | config-vlan-<VLAN-ID> | Administrators or local user group members with execution rights for this command. |

# show capacities-status vlan-count

```
show capacities-status vlan-count
```

## Description

Shows the number of VLANs present on the switch and the maximum number of VLANs allowed on the switch.

## Example

Showing switch VLAN capacity status:

```
show capswitch# show capacities-status vlan-count
System Capacities: Filter VLAN count
Capacities Name Value Maximum

Maximum number of VLANs currently configured 1 xxxx
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

# show capacities svi-count

show capacities svi-count

## Description

Shows the maximum number of SVIs supported by the switch. The value displayed in the output will vary depending upon switch model and version of AOS-CX. For details on SVI capacity for your switch model, refer to the **Capacities** section of the AOS-CX release notes.

## Examples

Showing HPE Aruba Networking SVI capacity. The actual value displayed in the output will vary, depending upon switch model and version of AOS-CX. For details on SVI capacity for your switch model, refer to the **Capacities** section of the AOS-CX release notes.

```
switch# show capacities svi-count
System Capacities: Filter SVI count
Capacities Name Value

Maximum number of SVIs supported in the system <value>
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show capacities vlan-count

show capacities vlan-count

### Description

Shows the maximum number of VLANs allowed on the switch.

### Example

Showing switch VLAN capacity:

```
show capswitch# show capacities vlan-count
System Capacities: Filter VLAN count
Capacities Name Value

Maximum number of VLANs supported in the system 4094
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show capacities-status vlan-translation

show capacities-status vlan-translation

### Description

Shows the number of VLAN translation rules present on the switch and the maximum number of VLAN translation rules allowed on the switch. The maximum number of VLAN translation rules allowed are:

- For 6300, 6400, 8100, 8360, 9300, 9300S and 10040 Switch series, 4000 rules
- .

### Example

Showing switch VLAN translation rules capacity:

```
switch(config-vlan-100)# show capacities vlan-translation
System Capacities: Filter VLAN Translation
Capacities Name Value

Maximum number of VLAN Translation rules supported
switch(config-vlan-100)#
switch(config-vlan-100)#
switch(config-vlan-100)#
switch(config-vlan-100)#
switch(config-vlan-100)# show capacities-st vlan-translation

System Capacities Status: Filter VLAN Translation
Capacities Status Name Value Maximum

Number of VLAN Translation rules currently configured 1
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show system internal-vlan-range

show system internal-vlan-range

### Description

Shows the VLAN range reserved for internal use.

### Examples

Showing reserved VLANs:



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## show vlan

show vlan [<VLAN-ID>] [vsx-peer]

### Description

Displays configuration information for all VLANs or a specific VLAN.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <VLAN-ID> | Specifies a VLAN ID.                                                                                                                                                                                                             |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Displaying configuration information for VLAN 2:

```
switch# show vlan 2
```

| VLAN | Name      | Status | Reason | Type   | Interfaces        |
|------|-----------|--------|--------|--------|-------------------|
| 2    | UserVLAN1 | up     | ok     | static | 1/1/1,1/1/3,1/1/5 |

Displaying configuration information for all defined VLANs:

```
switch# show vlan
```

| VLAN | Name           | Status | Reason     | Type   | Interfaces              |
|------|----------------|--------|------------|--------|-------------------------|
| -    |                |        |            |        |                         |
| 1    | DEFAULT_VLAN_1 | up     | ok         | static | 1/1/3-1/1/4             |
| 2    | UserVLAN1      | up     | ok         | static | 1/1/1,1/1/3,1/1/5       |
| 3    | UserVLAN2      | up     | ok         | static | 1/1/2-1/1/3,1/1/5-1/1/6 |
| 5    | UserVLAN3      | up     | ok         | static | 1/1/3                   |
| 10   | TestNetwork    | up     | ok         | static | 1/1/3,1/1/5             |
| 11   | VLAN11         | up     | ok         | static | 1/1/3                   |
| 12   | VLAN12         | up     | ok         | static | 1/1/3,1/1/6,lag1-lag2   |
| 13   | VLAN13         | up     | ok         | static | 1/1/3,1/1/6             |
| 14   | VLAN14         | up     | ok         | static | 1/1/3,1/1/6             |
| 20   | ManagementVLAN | down   | admin_down | static | 1/1/3,1/1/10            |



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vlan port

```
show vlan port <INTERFACE-ID> [vsx-peer]
```

### Description

Displays the VLANs configured for a specific layer 2 interface.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <INTERFACE-ID> | Specifies an interface ID. Format: <b>member/slot/port</b> .                                                                                                                                                                     |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Displaying the VLANs configured on interface **1/1/1**:

```
switch# show vlan port 1/1/1
```

| VLAN | Name      | Mode   | Mapping   |
|------|-----------|--------|-----------|
| 2    | UserVLAN1 | access | port      |
| 3    | UserVLAN2 | access | arp, ipv4 |
| 5    | UserVLAN5 | access | ipv6      |

Displaying the VLANs configured on interface **1/1/3**:

```
switch# show vlan port 1/1/3
```

| VLAN | Name | Mode | Mapping |
|------|------|------|---------|
|------|------|------|---------|

|     |                |                 |      |
|-----|----------------|-----------------|------|
| 1   | DEFAULT_VLAN_1 | native-untagged | port |
| 2   | UserVLAN1      | trunk           | port |
| 3   | UserVLAN2      | trunk           | port |
| 5   | UserVLAN3      | trunk           | port |
| 10  | TestNetwork    | trunk           | port |
| 11  | VLAN11         | trunk           | port |
| 12  | VLAN12         | trunk           | port |
| 13  | VLAN13         | trunk           | port |
| 14  | VLAN14         | trunk           | port |
| 20  | ManagementVLAN | trunk           | port |
| 30  | VLAN30         | trunk           | port |
| 40  | VLAN40         | trunk           | port |
| 50  | VLAN50         | trunk           | port |
| 100 | VLAN100        | trunk           | port |
| 200 | VLAN200        | trunk           | port |



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vlan summary

```
show vlan summary [vsx-peer]
```

### Description

Displays a summary of the VLAN configuration on the switch.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Displaying a summary of the VLAN configuration on the switch:



```
switch# show vlan summary
Number of existing VLANs: 11
Number of static VLANs: 11
Number of dynamic VLANs: 0
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vlan translation

```
show vlan translation [interface <INTERFACE-NAME>] [vsx-peer]
```

## Description

Shows a summary of all VLAN translations rules defined on the switch, or the rules defined for a specific interface.

| Parameter                  | Description                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface <INTERFACE-NAME> | Specifies the name of a layer 2 interface. Format: <b>member/slot/port</b> .                                                                                                                                                     |
| vsx-peer                   | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Displaying a summary of all VLAN translations rules defined on the switch:

```
switch# show vlan translation

Interface VLAN-1 VLAN-2

1/1/5 10 20
1/1/5 30 40
1/1/5 50 100
```

```
1/1/6 100 200

Total number of translation rules : 4
```

Displaying a summary of all VLAN translation rules defined on interface **1/1/5**:

```
switch# show vlan translation interface 1/1/5

Interface VLAN-1 VLAN-2

1/1/5 10 20
1/1/5 30 40
1/1/5 50 100
```

Displaying VLAN translation information when VSX peer is configured:

```
switch(config-if)# show vlan translation vsx-peer

Interface VLAN-1 VLAN-2

1/3/1 10 20
Total number of translation rules : 1
```

Displaying VLAN translation information when VSX peer is not configured:

```
switch(config-if)# show vlan translation vsx-peer
VSX is not configured
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vlan translation pending

show vlan translation pending

## Description

Shows a list of pending VLAN translation rules.

## Examples

Displaying a list of VLAN translations rules pending on the switch:

```
switch# show vlan translation pending

Interface VLAN-1 VLAN-2

1/1/5 10 20
1/1/5 30 40
1/1/5 50 100
1/1/6 100 200

Total number of VLAN translation rules that are pending: 4
```

Displaying the output when there are no VLAN translation rules in the pending list:

```
switch# show vlan translation interface 1/1/5
No pending VLAN translation rules
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.08 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vlan voice

show vlan voice

### Description

Displays the voice VLAN list showing the VLAN ID, name, operational state of the VLAN, and the interfaces associated with the VLAN.

### Example

Displaying the voice VLANs list :

```
switch# show vlan voice
```

```

VLAN Name Status Type Interfaces

10 TestNetwork up static 1/1/3,1/1/5
```

Displaying the information when voice VLANs are not configured:

```
switch# show vlan voice
Voice VLAN not configured
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# shutdown

```
shutdown
no shutdown
```

## Description

Disables a VLAN. (By default, a VLAN is automatically enabled when it is created with the **vlan** command.)

The **no** form of this command enables a VLAN.

## Examples

Enabling VLAN 20:

```
switch(config)# vlan 20
switch(config-vlan-20)# no shutdown
```

Disabling VLAN 20:

```
switch(config)# vlan 20
switch(config-vlan-20)# shutdown
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context       | Authority                                                                          |
|---------------|-----------------------|------------------------------------------------------------------------------------|
| All platforms | config-vlan-<VLAN-ID> | Administrators or local user group members with execution rights for this command. |

# system internal-vlan-range

```
system internal-vlan-range {<VLAND-ID>-<VLAN-ID> | none} [confirm]
no system internal-vlan-range {<VLAND-ID>-<VLAN-ID> | none} [confirm]
```

## Description

Configures the VLAN range reserved for internal use for route-only ports and LAGs. The internal VLAN range cannot include any VLANs that are already in use.

If the number of internal VLANs is less than the number of route-only ports and LAGs, some ports will be blocked and unable to be used. When the internal VLAN range is modified, traffic on route-only ports and LAGs is briefly interrupted while they are moved to the new range.

The **no** form of this command sets the range to the default range:

- 9300/9300S Switch series: 4041 to 4094

| Parameter            | Description                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <VLAND-ID>-<VLAN-ID> | Specifies the starting and ending VLAN number for the range. The reserved range must be between 2 and 4094 and cannot exceed 256 VLANs. |
| none                 | Do not reserve any internal VLANs.                                                                                                      |
| confirm              | Automatically acknowledge warning and skip confirmation prompt.                                                                         |

## Examples

Setting a new internal VLAN range:

```
switch(config)# system internal-vlan-range 3041-3094
This will briefly interrupt traffic.

Continue (y/n)?
```

Setting a new internal VLAN range, skipping the prompt:

```
switch(config)# system internal-vlan-range 3041-3094 confirm
```

Removing all internal VLANs:

```
switch(config)# system internal-vlan-range none
```

Removing all internal VLANs when some are in use:

```
switch(config)# system internal-vlan-range none
All route-only ports and LAGs will be blocked.

Continue (y/n)?
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## trunk-dynamic-vlan-include

```
trunk-dynamic-vlan-include
no trunk-dynamic-vlan-include
```

### Description

Indicates if dynamically learned VLANs from MVRP and port-access should be included or excluded on ports configured with **vlan trunk allowed all**. By default, dynamic VLANs are not included in the trunk allowed list. This command is used at the system-level.

The **no** form of this command disables the inclusion of dynamic VLANs in the VLANs table. This is the default.

## Examples

Including the dynamic VLANs in the VLAN table:

```
switch(config)# trunk-dynamic-vlan-include
```

Disabling the inclusion of dynamic VLANs in the VLAN table (default):

```
switch(config)# no trunk-dynamic-vlan-include
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.08   | Command introduced |

## Command Information

| Platforms     | Command context     | Authority                                                                          |
|---------------|---------------------|------------------------------------------------------------------------------------|
| All platforms | <code>config</code> | Administrators or local user group members with execution rights for this command. |

## uufb

uufb  
no uufb

### Description

Enables the Unknown Unicast Flood Block (UUFB) feature on a physical interface. When this feature is enabled on a physical interface, unknown unicast packets are blocked from egressing the physical interface. This feature is disabled by default.



UUFB can be enabled only on the physical interface.

UUFB cannot be enabled on:

- Routed interface
- LAGs
- VSX inter-switch link
- Interface used as an ISL

## Examples

Enabling UUFB on an L2 access port:

```
switch(config)# interface 1/1/1
switch(config-if)# vlan access 1
switch(config-if)# uufb
```

Enable UUFb on an L2 trunk port:

```
switch(config)# interface 1/1/1
switch(config-if)# vlan trunk allowed all
switch(config-if)# uufb
```

Disabling UUFb on an L2 access or trunk port:

```
switch(config-if)# no uufb
```

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.11   | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

# vlan

```
vlan <VLAN-LIST>
no vlan <VLAN-LIST>
```

## Description

Creates a VLAN and changes to the **config-vlan-id** context for the VLAN. By default, the VLAN is enabled. To disable a VLAN, use the **shutdown** command.

If the specified VLAN exists, this command changes to the **config-vlan-id** context for the VLAN. If a range of VLANs is specified, the context does not change.



VLANs used for internal purposes using the command **system internal vlan range** cannot be used for any other (L2) purposes.

The **no** form of this command removes a VLAN. VLAN 1 is the default VLAN and cannot be deleted.

| Parameter   | Description                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| <VLAN-LIST> | Specifies a single ID, or a series of IDs separated by commas (2, 3, 4), dashes (2-4), or both (2-4,6). Range: 1 to 4040. |

## Examples



### Creating VLAN 20:

```
switch(config)# vlan 20
switch(config-vlan-20)#
```

### Removing VLAN 20:

```
switch(config)# no vlan 20
```

### Creating VLANs 2 to 8 and 10:

```
switch(config)# vlan 2-8,10
```

### Removing VLANs 2 to 8 and 10:

```
switch(config)# no vlan 2-8,10
```

### Creating a VLAN which is already configured as an internal VLAN:

```
switch(config)# vlan 3001
Ignoring the operation on internal VLAN(s) 3001.
```

### Deleting an unconfigured VLAN which is already configured as internal VLAN:

```
switch(config)# no vlan 300
Ignoring the operation for non-configured VLAN(s) 300.
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## vlan access

```
vlan access <VLAN-ID>
no vlan access [<VLAN-ID>]
```

## Description

Creates an access interface and assigns an VLAN ID to it. Only one VLAN ID can be assigned to each access interface.

VLANs can only be assigned to non-routed (Layer 2) interfaces. All interfaces are non-routed (Layer 2) by default when created. Use **routing** and **no routing** commands to move ports between Layer 3 and Layer 2 interfaces.

The **no** form of this command removes an access VLAN from the interface in the current context and sets it to the default VLAN ID of 1.

## Command context

| Parameter                    | Description                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;VLAN-ID&gt;</code> | Specifies a single ID, or a series of IDs separated by commas (2, 3, 4), dashes (2-4), or both (2-4,6). Range: 1 to 4040. |

## Examples

Configuring interface **1/1/2** as an access interface with VLAN ID set to **20**:

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan access 20
```

Removing VLAN ID **20** from interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan access 20
```

or:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan access
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

# vlan protocol

```
vlan protocol <PROTOCOL_NAME> <VLAN-ID>
no vlan protocol <PROTOCOL_NAME> <VLAN-ID>
```

## Description

Adds protocol mapping to a VLAN on an interface.

The **no** form of this command removes protocol mapping from the VLAN on an interface.

| Parameter       | Description                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <VLAN-ID>       | Specifies a VLAN ID. Range: 2 to 4094.                                                                                                                                                       |
| <PROTOCOL_NAME> | Specifies the protocol that the VLAN is bound to for a given interface. Options are: <b>appletalk</b> , <b>arp</b> , <b>ip</b> , <b>ipv6</b> , <b>ipx</b> , <b>netbui</b> , and <b>sna</b> . |

## Usage

- This command is only applicable to access ports.
- Protocol VLAN should be different from access VLANs.
- VLAN should be configured on the switch.
- Routing must be disabled on the interface.
- Interface must be a physical or LAG interface.
- The same protocol-mapped VLAN is recommended for ARP and IPv4 protocols to avoid IPv4 traffic loss.

## Examples

Assigning a protocol mapping to a VLAN on an interface:

```
switch(config)# interface 1/1/2
switch(config-if)# vlan protocol ip 10
```

Assigning a protocol mapping to a VLAN on a LAG interface:

```
switch(config)# interface lag 2
switch(config-lag-if)# vlan protocol ipv6 10
```

Removing a protocol mapping from a VLAN on an interface:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan protocol ipv6 10
```

Removing a protocol mapping from a VLAN on a LAG interface:

```
switch(config)# interface lag 2
switch(config-lag-if)# no vlan protocol ipv6 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification                                                                                              |
|------------------|-----------------------------------------------------------------------------------------------------------|
| 10.14            | Replaced the <b>ipv4</b> parameter with the <b>ip</b> parameter. The <b>ipv4</b> parameter is deprecated. |
| 10.07 or earlier | --                                                                                                        |

## Command Information

| Platforms     | Command context            | Authority                                                                          |
|---------------|----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if<br>config-lag-if | Administrators or local user group members with execution rights for this command. |

# vlan translate

```
vlan translate <VLAN-1> <VLAN-2>
no vlan translate <VLAN-1> <VLAN-2>
```

## Description

Defines a bidirectional VLAN translation rule that maps an original VLAN ID (VLAN-1) to a translated internal VLAN ID (VLAN-2) on a LAG or layer 2 interface. Applies to both incoming and outgoing traffic. On the HPE Aruba Networking 8320, 8325, 8325H, and 9300/9300S Switch Series: Along with translated and native VLANs, VLAN trunk allowed VLANs are also respected and traffic is allowed. The **no** form of this command removes an existing VLAN translation rule on the current interface.



VLAN translation and MVRP cannot be enabled on the same interface.

A translated VLAN must be present on the switch before the rule is created; the original VLAN need not be present.

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| <VLAN-1>  | Specifies the number of an origin VLAN. Range: 1 - 4040.    |
| <VLAN-2>  | Specifies the number of a translated VLAN. Range: 1 - 4040. |

## Usage

- This configuration can be applied only on layer 2 trunk ports.
- Routing must be disabled on the interface.
- Interface must be a layer 2 physical or LAG interface.

- Maximum unique VLAN translation rules supported on the HPE Aruba Networking 9300/9300S Switch Series—10000

## Examples

Translates origin VLAN **200** to translated VLAN **20** on interface **1/1/2**.

```
switch(config)# vlan 20
switch(config-vlan-20)# exit
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 20
switch(config-if)# vlan translate 200 20
```

Translates origin VLANs **100** and **300** to translated VLANs **10** and **20** on interface **1/1/2**.

```
switch(config)# vlan 10,30
switch(config-vlan-20)# exit
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10,30
switch(config-if)# vlan translate 100 10
switch(config-if)# vlan translate 300 30
```



Though VLAN translation is not supported on Native VLAN configurations, a translation rule will be created to ensure VLAN translation works when the native VLAN is updated. These rules appear in the output of the **show running-config** command, though they are not operational.

```
(config)# interface 1/1/4
switch (config-if)# vlan translate 10 2
Warning: Operation not allowed on native VLAN 1
switch(config-if)# show runing-config current-context
interface 1/1/1
no shutdown
no routing
vlan trunk native 1
vlan trunk allowed all
vlan translate 1 2 <<< non-functional translation rules
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification                               |
|------------------|--------------------------------------------|
| 10.16.1000       | Support added for the 8325H Switch Series. |
| 10.07 or earlier | --                                         |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if       | Administrators or local user group members with execution rights for this command. |

## vlan trunk allowed

```
vlan trunk allowed [<VLAN-LIST> | all]
no vlan trunk allowed [<VLAN-LIST>]
```

### Description

Assigns a VLAN ID to a trunk interface. Multiple VLAN IDs can be assigned to a trunk interface. These VLAN IDs define which VLAN traffic is allowed across the trunk interface.

VLANs can only be assigned to non-routed (Layer 2) interfaces. All interfaces are non-routed (Layer 2) by default when created. Use **routing** and **no routing** commands to move ports between Layer 3 and Layer 2 interfaces.

The **no** form of this command removes one or more VLAN IDs from a trunk interface. When the last VLAN is removed from a trunk interface, the interface continues to operate in trunk mode, and will trunk all the VLANs currently defined on the switch, and any new VLANs defined in the future. To disable the trunk interface, use the command shutdown.

| Parameter   | Description                                                                                                                                   |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <VLAN-LIST> | Specifies a single ID, or a series of IDs separated by commas (2, 3, 4), dashes (2-4), or both (2-4,6). Range: 1 to 4040.                     |
| all         | Configures the trunk interface to allow all the VLANs currently configured on the switch and any new VLANs that are configured in the future. |

### Examples

Assigning VLANs **2, 3**, and **4** to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 2,3,4
```

Assigning VLAN IDs **2** to **8** to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 2-8
```

Assigning VLAN IDs **2** to **8** and **10** to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 2-8,10
```

Removing VLAN IDs **2, 3**, and **4** from trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan trunk allowed 2,3,4
```

Removing all VLANs assigned to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan trunk allowed 2
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## vlan trunk native

```
vlan trunk native <VLAN-ID>
no vlan trunk native [<VLAN-ID>]
```

### Description

Assigns a native VLAN ID to a trunk interface. By default, VLAN ID 1 is assigned as the native VLAN ID for all trunk interfaces. VLANs can only be assigned to a non-routed (layer 2) interface or LAG interface. Only one VLAN ID can be assigned as the native VLAN.



When a native VLAN is defined, the switch automatically executes the **vlan trunk allowed all** command to ensure that the default VLAN is allowed on the trunk. To only allow specific VLANs on the trunk, issue the **vlan trunk allowed** command specifying only specific VLANs.

The **no** form of this command removes a native VLAN from a trunk interface and assigns VLAN ID 1 as its native VLAN.

| Parameter | Description                            |
|-----------|----------------------------------------|
| <VLAN-ID> | Specifies a VLAN ID. Range: 1 to 4040. |

## Examples

Assigning native VLAN ID **20** to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk native 20
```

Removing native VLAN **20** from trunk interface **1/1/2** and returning to the default VLAN 1 as the native VLAN.

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan trunk native 20
```

or:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan trunk native
```

Assigning native VLAN ID **20** to trunk interface **1/1/2** and then removing it from the list of allowed VLANs. (Only allow VLAN 10 on the trunk.)

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk native 20
switch(config-if)# vlan trunk allowed 10
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## vlan trunk native tag

```
vlan trunk native <VLAN-ID> tag
no vlan trunk native <VLAN-ID> tag
```

## Description

Enables tagging on a native VLAN. Only incoming packets that are tagged with the matching VLAN ID are accepted. Incoming packets that are untagged are dropped except for BPDUs. Egress packets are tagged.



The **no** form of this command removes tagging on a native VLAN.

| Parameter | Description                                       |
|-----------|---------------------------------------------------|
| <VLAN-ID> | Specifies the number of a VLAN. Range: 1 to 4040. |

## Examples

Enabling tagging on native VLAN **20** on trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no routing
switch(config-if)# vlan trunk native 20
switch(config-if)# vlan trunk native 20 tag
```

Removing tagging on native VLAN **20** assigned to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no vlan trunk native 20 tag
```

Enabling tagging on native VLAN **20** assigned to LAG trunk interface **2**:

```
switch(config)# interface lag 2
switch(config-if)# no routing
switch(config-lag-if)# vlan trunk native 20
switch(config-lag-if)# vlan trunk native 20 tag
```



For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config-if       | Administrators or local user group members with execution rights for this command. |

## voice

voice  
no voice

## Description

Configures a VLAN as a voice VLAN.

The **no** form of this command removes voice configuration from a VLAN.

## Examples

Configuring VLAN 10 as a voice VLAN:

```
switch(config)# vlan 10
switch(config-vlan-10)# voice
```

Removing voice from VLAN 10:

```
switch(config-vlan-10)# no voice
```



---

For more information on features that use this command, refer to the Layer 2 Bridging Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                     | Authority                                                                          |
|---------------|-------------------------------------|------------------------------------------------------------------------------------|
| All platforms | config-vlan- <i>&lt;VLAN-ID&gt;</i> | Administrators or local user group members with execution rights for this command. |

### ip route vrf

```
ip route <DEST-IPV4-ADDR>/<MASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
 vrf <VRF-NAME> [name <WORD>]
no ip route <DEST-IPV4-ADDR>/<MASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
 vrf <VRF-NAME> [name <WORD>]
```

#### Description

Adds the destination IPv4 static route on the specified VRF. If no <VRF-NAME> is specified the route is applied to the default VRF.

The **no** form of this command removes the IPv4 static route from the VRF.

| Parameter          | Description                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <DEST-IPV4-ADDR>   | Specifies the route destination in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.            |
| <MASK>             | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 128. |
| <NEXT-HOP-IP-ADDR> | Specifies the next hop in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255.                     |
| <INTERFACE>        | Specifies the next hop as an outgoing interface.                                                                                |
| nullroute          | Silently discards packets to the destined route.                                                                                |
| reject             | Discards packets to the destined route and returns an ICMP error to the sender.                                                 |
| vrf <VRF-NAME>     | Specifies a VRF name.                                                                                                           |
| name <WORD>        | Assigns a name to the destination route. Range: 1 to 64 characters.                                                             |

#### Examples

```
switch(config)# ip route 20.0.0.0/8 10.20.30.44 vrf myvrf
switch(config)# ip route 20.1.2.0/24 1/1/30 vrf myvrf
switch(config)# ip route 1.2.3.4/32 nullroute vrf myvrf
switch(config)# ip route 1.2.3.4/32 reject vrf myvrf
switch(config)# ip route 20.0.4.0/24 10.0.0.2 vrf test name VRF-Management
```

```
switch(config)# no ip route 20.0.0.0/8 10.20.30.44 vrf myvrf
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                              |
|------------------|-------------------------------------------|
| 10.17            | The <b>name</b> parameter was introduced. |
| 10.10            | Inclusive language update.                |
| 10.07 or earlier | --                                        |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## ipv6 route gc interval

```
ipv6 route-gc-interval <INTERVAL>
no ipv6 route-gc-interval
```

### Description

Sets the garbage collection interval timer to remove invalid or old route entries from kernel route cache. The **no** form of this command resets the garbage collection interval timer to default (30 seconds).

| Parameter  | Description                                                        |
|------------|--------------------------------------------------------------------|
| <INTERVAL> | Specifies time interval in seconds. Range: 30 to 600. Default: 30. |

### Examples

Setting garbage collection interval timer to 300:

```
switch(config)# ipv6 route-gc-interval 300
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release | Modification       |
|---------|--------------------|
| 10.10   | Command introduced |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | config          | Administrators or local user group members with execution rights for this command. |

## ipv6 route vrf

```

ipv6 route <DEST-IPV6-ADDR>/<PREFIX> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
vrf <VRF-NAME> [name <WORD>]
no ipv6 route <DEST-IPV6-ADDR>/<PREFIX> [<NEXT-HOP-IP-ADDR>|<INTERFACE>|reject|nullroute]
vrf <VRF-NAME> [name <WORD>]

```

### Description

Adds an IPv6 static route in the specified VRF. If no *<VRF-NAME>* is specified it is added to the default VRF.

The **no** form of this command removes an IPv6 static route from the VRF.

| Parameter                       | Description                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;DEST-IPV6-ADDR&gt;</i>   | Specifies an IP address in IPv6 format ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> is a hexadecimal number from 0 to F. |
| <i>&lt;MASK&gt;</i>             | Specifies the number of bits in the address mask in CIDR format ( <b>x</b> ), where <b>x</b> is a decimal number from 0 to 128.                |
| <i>&lt;NEXT-HOP-IP-ADDR&gt;</i> | Specifies the next hop in IPv6 format ( <b>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx</b> ), where <b>x</b> is a hexadecimal number from 0 to F.  |
| <i>&lt;INTERFACE&gt;</i>        | Specifies the next hop as an outgoing interface.                                                                                               |
| nullroute                       | Specifies that packets matching the destination prefix are silently discarded and no ICMP error notification is sent to the sender.            |
| reject                          | Specifies that packets matching the destination prefix are discarded and an ICMP error notification is sent to the sender.                     |
| vrf <i>&lt;VRF-NAME&gt;</i>     | Specifies the name of a VRF. Default: default.                                                                                                 |
| name <i>&lt;WORD&gt;</i>        | Assigns a name to the destination route. Range: 1 to 64 characters.                                                                            |

### Examples

```

switch(config)# ipv6 route 120::/124 121::2 vrf test
switch(config)# ipv6 route 121::/124 1/1/9 vrf test
switch(config)# ipv6 route 122::/124 nullroute vrf test
switch(config)# ipv6 route 123::/124 reject vrf test
switch(config)# ipv6 route 124::/124 121::3 vrf test name IPv6-VRF-Link

```

```

switch(config)# no ipv6 route 120::/124 121::2 vrf test

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                              |
|------------------|-------------------------------------------|
| 10.17            | The <b>name</b> parameter was introduced. |
| 10.10            | Inclusive language update.                |
| 10.07 or earlier | --                                        |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## show ip route

```
show ip route [<A.B.C.D> | <A.B.C.D/M> | all-vrfs | bgp | connected | local | ospf |
static | summary | vrf <VRF-NAME> [vsx-peer] | protected]
```

## Description

Displays IP route tables.

| Parameter      | Description                                                                            |
|----------------|----------------------------------------------------------------------------------------|
| <A.B.C.D>      | Display longest prefix match.                                                          |
| <A.B.C.D/M>    | Display exact route match.                                                             |
| all-vrfs       | Display information for all VRFs.                                                      |
| bgp            | Display bgp routes only.                                                               |
| connected      | Display connected routes only.                                                         |
| local          | Display local routes only.                                                             |
| ospf           | Display ospf routes only.                                                              |
| protected      | Display protected routes only.                                                         |
| static         | Display static routes only.                                                            |
| summary        | Display the aggregate count of routes per routing protocol.                            |
| vrf <vrf-name> | Specify a VRF by VRF name (if no <VRF-NAME> is specified, the default VRF is implied). |

## Examples

## Showing IP routes:

```
dut1# show ip route all-vrfs

Displaying ip routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
 R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
 IA - OSPF internal area, E1 - OSPF external type 1
 E2 - OSPF external type 2
FRR: + - Backup Nexthop
 * - data obtainable via 'show bgp ip unicast A.B.C.D/M'

VRF: 1

Prefix Nexthop Interface VRF(egress) Origin/ Distance/ Age
 Type Type Metric

--
1.1.1.0/24 - 1/1/22 - C [0/0] -
1.1.1.1/32 - 1/1/22 - L [0/0] -
1.1.2.0/24 - 1/1/23 - C [0/0] -
1.1.2.1/32 - 1/1/23 - L [0/0] -
1.1.5.0/24 - 1/1/25 - C [0/0] -
1.1.5.1/32 - 1/1/25 - L [0/0] -
200.1.0.0/24 1.1.2.2 1/1/23 - B/E [20/0] 00h:00m:13s
 1.1.1.2+ 1/1/22 - B/* [*/0] 00h:00m:13s
200.1.1.0/24 1.1.2.2 1/1/23 - B/E [20/0] 00h:00m:13s
 1.1.1.2+ 1/1/22 - B/* [*/0] 00h:00m:13s
200.1.2.0/24 1.1.2.2 1/1/23 - B/E [20/0] 00h:00m:13s
 1.1.1.2+ 1/1/22 - B/* [*/0] 00h:00m:13s
200.1.3.0/24 1.1.2.2 1/1/23 - B/E [20/0] 00h:00m:13s
 1.1.1.2+ 1/1/22 - B/* [*/0] 00h:00m:13s
200.1.4.0/24 1.1.2.2 1/1/23 - B/E [20/0] 00h:00m:13s
 1.1.1.2+ 1/1/22 - B/* [*/0] 00h:00m:13s
Total Route Count : 11
```

## Showing ip protected routes:

```
switch# show ip route protected
all-vrfs all vrf information
vrf Specify the VRF name
<cr>
```

## Showing protected routes for all vrfs:



---

Protected routes are only supported on the 9300 Switch Series.

---

```
switch# show ip route protected all-vrfs

Displaying ip routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
 R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
```

```

IA - OSPF internal area, E1 - OSPF external type 1
E2 - OSPF external type 2
FRR:
+ - Backup Nexthop
* - data obtainable via 'show bgp ip unicast A.B.C.D/M'

VRF: default

Prefix Nexthop Interface VRF(egress) Origin/ Distance/ Age
 Type

--
120.120.120.0/24 110.110.110.1 vlan20 - O [110/120]
03h:35m:55s
 130.130.130.1+ vlan22 - B/* [*/120] 03h:35m:55s
140.140.140.0/24 130.130.130.1 vlan22 - O [110/130]
03h:25m:13s
 110.110.110.1+ vlan20 - B/* [*/130] 03h:25m:13s
211.0.0.0/24 110.110.110.1 vlan20 - O [110/122]
03h:25m:13s
 130.130.130.1+ vlan22 - B/* [*/122] 03h:25m:13s

VRF: red

150.150.150.0/24 120.120.120.1 vlan21 - O [110/120]
03h:35m:55s
 140.140.140.1+ vlan23 - B/* [*/120] 03h:35m:55s

Total Route Count : 4

```

Showing protected routes for a specific vrf, **vrf red**:

```

switch# show ip route protected vrf red

Displaying ip routes selected for forwarding
Origin Codes: C - connected, S - static, L - local
 R - RIP, B - BGP, O - OSPF, D - DHCP
Type Codes: E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
 IA - OSPF internal area, E1 - OSPF external type 1
 E2 - OSPF external type 2
FRR:
+ - Backup Nexthop
* - data obtainable via 'show bgp ip unicast A.B.C.D/M'

VRF: red

Prefix Nexthop Interface VRF(egress) Origin/ Distance/ Age
 Type

--
150.150.150.0/24 121.120.120.1 vlan21 - O [110/120]
03h:35m:55s
 141.140.140.1+ vlan23 - B/* [*/120] 03h:35m:55s

Total Route Count : 1

```

Show IP routes for a specific IP address:

```

dut1# show ip route 200.1.0.0/24 vrf 1

VRF: 1

```



```

Prefix : 200.1.0.0/24 VRF(egress)
: -
Nexthop : 1.1.2.2 Interface
: 1/1/6
Origin : bgp Type
: bgp_ext
Distance : 20 Metric
: 0
Age : 00h:00m:22s Tag
: 0
Encap Type : - Encap Details
: -
Nexthop Type : Primary

Prefix : 200.1.0.0/24 VRF(egress)
: -
Nexthop : 1.1.1.2 Interface
: 1/1/2
Origin : bgp Type
: *
Distance : * Metric
: 0
Age : 00h:00m:22s Tag
: 0
Encap Type : - Encap Details
: -
Nexthop Type : Backup

* - data for backup nexthop obtainable via 'show bgp ip unicast A.B.C.D/M'

```

Showing the ip route summary for all vrfs:

```

core1# show ip route summary all-vrfs

IP Route Table Summary

VRF name : red
Protocol Active Routes Protected Routes

connected 3 -
local 3 -
bgp 12 5

```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                                     |
|------------------|--------------------------------------------------|
| 10.14.1000       | Added protected paramater to 9300 Switch Series. |
| 10.07 or earlier | --                                               |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show ipv6 route

```
show ipv6 route [<X.X.X.X> | <X.X.X.X/M> | all-vrfs | bgp | connected | local | ospf |
static | summary | vrf <vrf-name>] [vsx-peer]
```

### Description

Displays IPv6 route tables.

| Parameter      | Description                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <X.X.X.X>      | Display exact route match.                                                                                                                                                                                                       |
| <X.X.X.X/M>    | Display exact route match.                                                                                                                                                                                                       |
| all-vrfs       | Display information for all VRFs.                                                                                                                                                                                                |
| bgp            | Display bgp routes only.                                                                                                                                                                                                         |
| connected      | Display connected routes only.                                                                                                                                                                                                   |
| local          | Display local routes only.                                                                                                                                                                                                       |
| ospf           | Display ospf routes only.                                                                                                                                                                                                        |
| static         | Display static routes only.                                                                                                                                                                                                      |
| summary        | Display the aggregate count of routes per routing protocol.                                                                                                                                                                      |
| vrf <vrf-name> | Specify a VRF by VRF name (if no <VRF-NAME> is specified, the default VRF is implied).                                                                                                                                           |
| vsx-peer       | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

Showing IPv6 route tables:

```
switch# show ipv6 route

Displaying ipv6 routes selected for forwarding

'[x/y]' denotes [distance/metric]

1000::/64, vrf default
 via vlan2, [0/0], connected
1000::1/128, vrf default
 via vlan2, [0/0], local
```

```
2000::/64, vrf default
 via vlan2, [1/0], static
2001::/64, vrf default
 via 1000::2, [1/0], static
3000:2301::/64, vrf default
 nullroute, [1/0], static
4000:2301::/64, vrf default
 reject route, [1/0], static
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification               |
|------------------|----------------------------|
| 10.10            | Inclusive language update. |
| 10.07 or earlier | --                         |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vrf

```
show vrf <VRF-NAME>
show vrf
```

### Description

Displays the status and attached interfaces for the specified VRF instance.

The **show vrf** command shows this information for all the VRFs.

| Parameter  | Description                                                       |
|------------|-------------------------------------------------------------------|
| <VRF-NAME> | Specifies the VRF name. Length: Up to 32 alphanumeric characters. |

### Examples

Showing VRF information for the test VRF:

```
switch# show vrf test
VRF Configuration:

VRF Name : test
 Interfaces Status

```

|        |    |
|--------|----|
| 1/1/29 | up |
| 1/1/30 | up |

Showing VRF information for all VRFs:

```
switch# show vrf
VRF Configuration:

VRF Name : default
Interfaces Status

VRF Name : red
Interfaces Status

1/1/32 up
VRF Name : test
Interfaces Status

1/1/29 up
1/1/30 up
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## vrf

```
vrf <VRF-NAME>
no vrf <VRF-NAME>
```

## Description

Creates a VRF instance named <VRF-NAME> and then enters its context. Use **default** for <VRF-NAME> to enter the default VRF configure context.

Except for the default VRF, the **no** form of the command deletes the named VRF instance and any IP configuration for interfaces or SVI linked to default VRF. The default VRF cannot be deleted and a warning is given if attempted. To erase the Route-Distinguisher and Route-Targets, enter the default VRF context and delete them manually one by one.

| Parameter                     | Description                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------|
| <code>&lt;VRF-NAME&gt;</code> | Specifies the VRF name. Range: Up to 32 alphanumeric characters. The <b>mgmt</b> VRF cannot be used. |

## Examples

Creating the VRF named **cust\_A** and then entering its context:

```
switch(config) # vrf cust_A
```

Entering the **default** VRF context:

```
switch(config) # vrf default
```

Deleting the VRF named **test**:

```
switch(config) # no vrf test
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                   |
|------------------|--------------------------------|
| 10.09            | Added default VRF information. |
| 10.07 or earlier | --                             |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## vrf attach

```
vrf attach <VRF-NAME>
no vrf attach <VRF-NAME>
```

### Description

Attaches the interface to the VRF with the name `<VRF-NAME>`. The command can be entered in several different command contexts.



The **no** form of the command detaches the interface from the named VRF and will remove all configurations from the interface and attach the interface to the default VRF. A warning message is displayed that prompts you whether to proceed: **All Layer 3 configurations associated with the VRF will be deleted. Continue (y/n)?**

| Parameter                     | Description                                                                 |
|-------------------------------|-----------------------------------------------------------------------------|
| <code>&lt;VRF-NAME&gt;</code> | Specifies the VRF name. Required. Length: Up to 32 alphanumeric characters. |

### Examples

```
switch(config)# interface 1/1/29
switch(config-if)# vrf attach test
```

```
switch(config)# vlan 3
switch(config-vlan)# exit
switch(config)# interface vlan 3
switch(config-if-vlan)# vrf attach test
```

```
switch(config)# vrf test
switch(config)# interface lag 3
switch(config-lag-if)# no shutdown
switch(config-lag-if)# vrf attach test
```

```
switch(config)# interface 1/1/29
switch(config-if)# no vrf attach test
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context                                               | Authority                                                                          |
|---------------|---------------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if<br>config-if-vlan<br>config-lag-if<br>config-gre-if | Administrators or local user group members with execution rights for this command. |

### address

```
address <IP-ADDR> [primary | secondary]
no address <IP-ADDR> [primary | secondary]
```

#### Description

Configures a primary or secondary IPv4 or IPv6 address for the VRRP group. To use secondary IP addresses in a VRRP group, you must first configure a primary IP address on the same group. A maximum of 16 IP addresses per IPv4 VRRP group and 8 IPv6 addresses per IPv6 VRRP group are supported.



Do not configure an IPv4 VRRP group using addresses from the /30, /31, and /32 subnets of the interface IP address.

16 Virtual IP addresses per IPv4 VR and 8 Virtual IP addresses per IPv6 VR are supported.



The total number of VIPs supported by a switch is:

- 1024 VIPs for IPv4 VRs
- 512 VIPs for IPv6 VRs

The **no** form of this command deletes a primary or secondary IPv4 or IPv6 address from the VRRP group.

| Parameter | Description                          |
|-----------|--------------------------------------|
| <IP-ADDR> | Configures the IPv4 or IPv6 address. |
| primary   | Configures a primary address.        |
| secondary | Configures a secondary address.      |

#### Examples

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# address 10.0.0.1 primary
```

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ipv6
switch(config-if-vrrp)# address fe80::1 primary
```

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# no address 10.0.0.1 primary

switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ipv6
switch(config-if-vrrp)# no address fe80::1 primary
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## authentication

```
authentication {text | md5} [{plaintext | ciphertext} <KEY>]
no authentication
```

### Description

This command enables authentication mode and the authentication key for VRRP groups on an interface. VRRP members or routers of the same VRRP group must use the same authentication mode and authentication key.

The no form of this command disables authentication mode and the authentication key for VRRP groups on an interface.

IPv4 VRRPv3 and IPv6 VRRPv3 do not support VRRP packet authentication. Authentication mode and key configuration take effect only in VRRPv2 (IPv4 only - RFC2338).

In VRRPv3, authentication mode and authentication key settings do not take effect because VRRP Authentication was removed from RFC5798.

VRRP provides the following authentication modes as described in RFC2338:

#### Simple authentication

The sender fills an authentication key into the VRRP packet and the receiver compares the received authentication key with its local authentication key.

If the two authentication keys match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and is discarded.





Authentication key text is sent in the clear and can be seen in a packet trace. This makes MD5 authentication more secure than text.

## MD5 authentication

The sender computes a digest for the packet that will be sent using the authentication key and MD5 algorithm, and saves the result in the VRRP packet.

The receiver performs the same operation with the authentication key and MD5 algorithm, and compares the result with the content in the authentication header. If the results match, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate and is discarded.

| Parameter  | Description                                              |
|------------|----------------------------------------------------------|
| text       | Configures the simple authentication type.               |
| md5        | Configures the MD5 (message-digest) authentication type. |
| plaintext  | Specifies that the key is provided as plaintext.         |
| ciphertext | Specifies that the key is provided as ciphertext.        |
| <KEY>      | Specifies the key in the chosen format.                  |



When the key is not provided on the command line, plaintext key prompting occurs upon pressing Enter. The entered key characters are masked with asterisks.

## Examples

Enabling VRRP authentication using MD5 with a provided plaintext key:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# version 2
switch(config-if-vrrp)# authentication md5 plaintext testvrrpkey
```

Enabling VRRP authentication using MD5 with a prompted plaintext key:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# version 2
switch(config-if-vrrp)# authentication md5
Enter the authentication key: *****
Re-Enter the authentication key: *****
```

Enabling VRRP authentication using MD5 with a provided ciphertext key:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# version 2
switch(config-if-vrrp)# authentication md5 ciphertext
AQBapfciFZ/P...biBAAAAOjc0a8=
```

Disabling VRRP authentication:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# version 2
switch(config-if-vrrp)# no authentication
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vrrp  | Administrators or local user group members with execution rights for this command. |

## bfd <IPV4-ADDR>

```
bfd <IPV4-ADDR>
no bfd <IPV4-ADDR>
```

### Description

Enables BFD under VRRP for the specified IP address. BFD is asynchronous and echo mode is supported.

The **no** form of this command disables BFD under VRRP for the specified IP address.

| Parameter   | Description                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <IPV4-ADDR> | Specifies the address on which to enable BFD in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. |

## Examples

Enabling BFD on the address **10.0.0.1** on VRRP **1**:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# bfd 10.0.0.1
```

Disabling BFD on the address **10.0.0.1** on VRRP **1**:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ipv4
```

```
switch(config-if-vrrp) # no bfd 10.0.0.1
```



For more information on features that use this command, refer to the High Availability Guide or IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vrrp  | Administrators or local user group members with execution rights for this command. |

## preempt

```
preempt
no preempt
```

## Description

Enables the preempt option. The default value is enabled. In default mode, a Standby router with a higher priority than another Standby that is operating as Active will take over the Active function.

Applies to VRRP Standby routers only and is used to minimize network disruption caused by unnecessary preemption of the Active operation among Standby routers.

The **no** form of this command disables the preempt option, thus preventing the higher-priority Standby from taking over the Active operation from a lower-priority Standby. This command does not prevent an owner router from resuming the Active function after recovering from being unavailable.

## Examples

```
switch(config) # interface 1/1/1
switch(config-if) # vrrp 1 address-family ip
switch(config-if-vrrp) # preempt
```

```
switch(config) # interface 1/1/1
switch(config-if) # vrrp 1 address-family ip
switch(config-if-vrrp) # no preempt
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## preempt delay minimum

```
preempt delay minimum <DELAY-IN-SECONDS>
no preempt delay minimum <DELAY-IN-SECONDS>
```

### Description

Sets the time in seconds (1-3600) that the router will wait before taking control of the virtual IP and starting to route packets.

The **no** form of this command sets the preempt delay for the VRRP group to the default preempt delay of 0 seconds.

The VRRP Preempt Delay Timer (PDT) allows admin users to configure a period of time before the VR takes control of the virtual IP address. It does not transition to the Active state until the timer period expires.

The timer value configured should be long enough to allow upper layer protocol to converge. The PDT is applied during initialization and down/up events of the router.

| Parameter          | Description                                                 |
|--------------------|-------------------------------------------------------------|
| <DELAY-IN-SECONDS> | Selects the time in seconds (1-3600). Default is 0 seconds. |

### Examples

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# preempt delay minimum 30

switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# no preempt delay
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## priority

```
priority <1-254>
no priority
```

### Description

Sets the priority for the VRRP group.

The **no** form of this command sets the priority for the VRRP group as default priority.

- The default value for non-Owner virtual routers is 100.
- The default value for Owner virtual router is 255, which cannot be changed.

### Examples

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# priority 150
```

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# no priority
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## router vrrp {enable | disable}

```
router vrrp {enable | disable}
no router vrrp {enable | disable}
```

## Description

Enables or disables VRRP protocol globally. You must globally enable the VRRP feature for VRRP virtual router.

**no router vrrp enable** disables VRRP protocol globally but does not remove all VRRP configurations.

**no router vrrp disable** enables VRRP protocol globally.

## Example

Enabling VRRP protocol globally:

```
switch(config)# router vrrp enable
```

Disable VRRP protocol globally:

```
switch(config)# router vrrp disable
```

Disable VRRP protocol globally:

```
switch(config)# no router vrrp enable
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## no router vrrp

```
no router vrrp
```

## Description

Removes VRRP configuration and VRRP global protocol. If **auto-confirm** is enabled or VRRP is not configured on any interface, this command will not ask for user confirmation.

## Examples

Removing VRRP configuration:

```
switch(config)# no router vrrp
All VRRP configuration will be deleted.
Do you want to continue (y/n)?
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# show track

```
show track [brief | <OBJECT-ID>]
```

## Description

Shows all or specific track object information.

| Parameter   | Description                                                    |
|-------------|----------------------------------------------------------------|
| brief       | Displays brief information about all or specific track objects |
| <OBJECT-ID> | Displays information about a specified track object (1-128)    |

## Examples

```
switch# show track
Track 1
 interface 1/1/1
 Interface is DOWN
```

```
switch# show track brief
Track Interface State
1 1/1/1 Down
2 None Down
3 1/1/2 Up
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show track brief

show track brief

### Description

Shows brief information for all track objects.

### Examples

Showing brief information for all track objects:

```
switch# show track brief
Track Interface State
1 1/1/1 Down
2 None Down
3 1/1/2 Up
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vrrp



```
show vrrp [brief | detail | interface <INTERFACE-NAME> | interface <LAG-NAME> | interface
<VLAN-NAME> | ip | ipv6 | statistics | statistics interface <INTERFACE-NAME> | statistics
interface <LAG-NAME> | statistics interface <VLAN-NAME>]
[vsx-peer]
```

## Description

Shows all VRRP virtual routers information.

| Parameter                             | Description                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| brief                                 | Displays brief output of all VRRP virtual routers<br>Keywords used in displayed information:<br>Grp: VRRP virtual router group ID.<br>A-F: Address Family.<br>Pri: Priority.<br>Time: Uptime of VRRP virtual router since it moved out of INIT state.<br>Pre: Preempt mode (Y is enabled, N if not enabled). |
| detail                                | Displays detailed output of all VRRP virtual routers                                                                                                                                                                                                                                                         |
| interface <INTERFACE-NAME>            | Displays VRRP information for a specific interface                                                                                                                                                                                                                                                           |
| interface <LAG-NAME>                  | Displays VRRP information for a specific LAG interface                                                                                                                                                                                                                                                       |
| interface <VLAN-NAME>                 | Displays VRRP information for a specific VLAN interface                                                                                                                                                                                                                                                      |
| ip                                    | Displays the IP address family                                                                                                                                                                                                                                                                               |
| ipv6                                  | Displays IPv6 address family                                                                                                                                                                                                                                                                                 |
| statistics                            | Displays VRRP statistics information for all interfaces                                                                                                                                                                                                                                                      |
| statistics interface <INTERFACE-NAME> | Displays VRRP statistics information for a specific interface                                                                                                                                                                                                                                                |
| statistics interface <LAG-NAME>       | Displays VRRP statistics information for a specific LAG interface                                                                                                                                                                                                                                            |
| statistics interface <VLAN-NAME>      | Displays VRRP statistics information for a specific VLAN interface                                                                                                                                                                                                                                           |
| vsx-peer                              | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                                                             |

## Examples

```
switch# show vrrp
VRRP is enabled

Interface 1/1/1 - Group 1 - Address-Family IPv

State is ACTIVE
State duration 56 mins 57.826 secs
Virtual IP address is 10.0.0.1
Virtual MAC address is 00:00:5e:00:01:01
```

```

Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
Active Router is 10.0.0.2 (local), priority is 100
Active Advertisement interval is 1000 msec
Active Down interval is unknown
Tracked object ID is 1, and state Down

Interface 1/1/2 - Group 1 - Address-Family IPv4
State is INIT (Interface Down)
State duration 45 mins 28.313 secs
Virtual IP address is no address
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
Active Router is unknown, priority is unknown
Active Advertisement interval is unknown
Active Down interval is unknown

Interface 1/1/2 - Group 1 - Address-Family IPv6
State is INIT (Group Disabled)
State duration 20 mins 19.794 secs
Virtual IP address is no address
Virtual secondary IP addresses:
 2201:13::110:4
Virtual MAC address is 00:00:5e:00:02:01
Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
Active Router is unknown, priority is unknown
Active Advertisement interval is unknown
Active Down interval is unknown

```

```
switch# show vrrp brief
```

VRRP is enabled

| Interface | Grp | A-F  | Pri | Time | Owner | Pre | State  | Active addr/Group addr   |
|-----------|-----|------|-----|------|-------|-----|--------|--------------------------|
| 1/1/1     | 1   | IPv4 | 100 | 0    | N     | Y   | ACTIVE | 10.0.0.2(local) 10.0.0.1 |
| 1/1/2     | 1   | IPv4 | 100 | 0    | N     | Y   | INIT   | AF-UNDEFINED no address  |
| 1/1/2     | 1   | IPv6 | 100 | 0    | N     | Y   | INIT   | AF-UNDEFINED no address  |

```
switch# show vrrp detail
```

VRRP is enabled

```

Interface 1/1/1 - VRRPv2 Statistics
 Invalid group ID packets received : 0
 Invalid version packets received : 0
 Invalid checksum packets received : 0

```

```

Interface 1/1/1 - VRRPv3 Statistics
 Invalid group ID packets received : 0
 Invalid version packets received : 0
 Invalid checksum packets received : 0

```

```

Interface 1/1/1 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 1 mins 35.486 secs
Virtual IP address is 10.0.0.1

```

```

Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1000 msec
Version 3
Preemption enabled
Priority is 100
Active Router is 10.0.0.2 (local), priority is 100
Active Advertisement interval is 1000 msec
Active Down interval is unknown
Tracked object ID is 1, and state Down
VRRPv3 Advertisements: sent 3931 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 3537
 IP address Owner conflicts: 0
 IP address configuration mismatch : 3537
 Advert Interval errors : 0
 Adverts received in Init state: 0
 Invalid group other reason: 0
Group State transition:
 Init to active: 0
 Init to standby: 2 (Last change Mon Jun 16 11:19:36.316 UTC)
 Standby to active: 2 (Last change Mon Jun 16 11:19:39.926 UTC)
 Active to standby: 0
 Active to init: 1 (Last change Mon Jun 16 11:17:49.978 UTC)
 Standby to init: 0

Interface 1/1/2 - VRRPv2 Statistics
 Invalid group ID packets received : 0
 Invalid version packets received : 0
 Invalid checksum packets received : 0

Interface 1/1/2 - VRRPv3 Statistics
 Invalid group ID packets received : 0
 Invalid version packets received : 0
 Invalid checksum packets received : 0

Interface 1/1/2 - Group 1 - Address-Family IPv4
 State is INIT (Interface Down)
 State duration 49 mins 23.507 secs
 Virtual IP address is no address
 Virtual MAC address is 00:00:5e:00:01:01
 Advertisement interval is 1000 msec
 Version 3
 Preemption enabled
 Priority is 100
 Active Router is unknown, priority is unknown
 Active Advertisement interval is unknown
 Active Down interval is unknown
 VRRPv3 Advertisements: sent 0 (errors 0) - rcvd 0
 VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
 Group Discarded Packets: 0
 IP address Owner conflicts: 0
 IP address configuration mismatch : 0
 Advert Interval errors: 0
 Adverts received in Init state: 0
 Invalid group other reason: 0
 Group State transition:
 Init to active: 0
 Init to standby: 0
 Standby to active: 0
 Active to standby: 0
 Active to init: 0
 Standby to init: 0

```

```
Interface 1/1/2 - Group 1 - Address-Family IPv6
State is INIT (Interface Down)
State duration 24 mins 14.988 secs
Virtual IP address is no address
Virtual secondary IP addresses:
 2201:13::110:4
Virtual MAC address is 00:00:5e:00:02:01
Advertisement interval is 1000 msec
Preemption enabled
Priority is 100
Active Router is unknown, priority is unknown
Active Advertisement interval is unknown
Active Down interval is unknown
VRRPv3 Advertisements: sent 0 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 0
 VRRPv2 incompatibility: 0
 IP address Owner conflicts: 0
 IP address configuration mismatch : 0
 Advert Interval errors : 0
 Adverts received in Init state: 0
 Invalid group other reason: 0
Group State transition:
 Init to active: 0
 Init to standby: 0
 Standby to active: 0
 Active to standby: 0
 Active to init: 0
 Standby to init: 0
```

```
switch# show vrrp interface 1/1/1
VRRP is enabled
```

```
Interface 1/1/1 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 11 mins 21.617 secs
Virtual IP address is 10.0.0.1
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1000 msec
Version 3
Preemption enabled
Priority is 100
Active Router is 10.0.0.2 (local), priority is 100
Active Advertisement interval is 1000 msec
Active Down interval is unknown
```

```
switch# show vrrp interface lag10
VRRP is enabled
```

```
Interface lag10 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 11 mins 21.617 secs
Virtual IP address is 10.0.0.1
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1000 msec
Version 3
Preemption enabled
Priority is 100
Active Router is 10.0.0.2 (local), priority is 100
```

```
Active Advertisement interval is 1000 msec
Active Down interval is unknown
```

```
switch# show vrrp interface vlan100
VRRP is enabled
```

```
Interface vlan100 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 11 mins 21.617 secs
Virtual IP address is 10.0.0.1
Virtual MAC address is 00:00:5e:00:01:01
Advertisement interval is 1000 msec
Version 3
Preemption enabled
Priority is 100
Active Router is 10.0.0.2 (local), priority is 100
Active Advertisement interval is 1000 msec
Active Down interval is unknown
```

```
switch# show vrrp statistics
```

```
VRRP is enabled
```

```
Interface 1/1/1 - VRRPv2 Statistics
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

```
Interface 1/1/1 - VRRPv3 Statistics
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

```
VRRP Statistics for interface 1/1/1 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 6 mins 55.006 secs
VRRPv3 Advertisements: sent 4288 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 3856
IP address Owner conflicts: 0
IP address configuration mismatch : 0
Advert Interval errors : 0
Adverts received in Init state: 0
Invalid group other reason: 0
Group State transition:
Init to active: 0
Init to standby: 2 (Last change Mon Jun 16 11:19:36.316 UTC)
Standby to active: 2 (Last change Mon Jun 16 11:19:39.926 UTC)
Active to standby: 0
Active to init: 1 (Last change Mon Jun 16 11:17:49.978 UTC)
Standby to init: 0
```

```
Interface 1/1/2 - VRRPv2 Statistics
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

```
Interface 1/1/2 - VRRPv3 Statistics
Invalid group ID packets received : 0
Invalid version packets received : 0
```

```

Invalid checksum packets received : 0

VRRP Statistics for Interface 1/1/2 - Group 1 - Address-Family IPv4
State is INIT (No Primary Group Address)
State duration 54 mins 43.027 secs
VRRPv3 Advertisements: sent 0 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 0
 IP address Owner conflicts: 0
 Invalid address count: 0
 IP address configuration mismatch : 0
 Advert Interval errors : 0
 Adverts received in Init state: 0
 Invalid group other reason: 0
Group State transition:
 Init to active: 0
 Init to standby: 0
 Standby to active: 0
 Active to standby: 0
 Active to init: 0
 Standby to init: 0

VRRP Statistics for Interface 1/1/2 - Group 1 - Address-Family IPv6
State is INIT (Interface Down)
State duration 29 mins 34.508 secs
VRRPv3 Advertisements: sent 0 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 0
 IP address Owner conflicts: 0
 IP address configuration mismatch : 0
 Advert Interval errors: 0
 Adverts received in Init state: 0
 Invalid group other reason: 0
Group State transition:
 Init to active: 0
 Init to standby: 0
 Standby to active: 0
 Active to standby: 0
 Active to init: 0
 Standby to init: 0

```

```

switch# show vrrp statistics interface 1/1/1

```

```

VRRP is enabled

```

```

Interface 1/1/1 - VRRPv2 Statistics
 Invalid group ID packets received : 0
 Invalid version packets received : 0
 Invalid checksum packets received : 0

```

```

Interface 1/1/1 - VRRPv3 Statistics
 Invalid group ID packets received : 0
 Invalid version packets received : 0
 Invalid checksum packets received : 0

```

```

VRRP Statistics for interface 1/1/1 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 6 mins 55.006 secs
VRRPv3 Advertisements: sent 4288 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 3856

```

```
IP address Owner conflicts: 0
IP address configuration mismatch : 0
Advert Interval errors : 0
Adverts received in Init state: 0
Invalid group other reason: 0
Group State transition:
Init to active: 0
Init to standby: 2 (Last change Mon Jun 16 11:19:36.316 UTC)
Standby to active: 2 (Last change Mon Jun 16 11:19:39.926 UTC)
Active to standby: 0
Active to init: 1 (Last change Mon Jun 16 11:17:49.978 UTC)
Standby to init: 0
```

```
switch# show vrrp statistics interface lag10
```

VRRP is enabled

Interface lag10 - VRRPv2 Statistics

```
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

Interface lag10 - VRRPv3 Statistics

```
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

VRRP Statistics for interface lag10 - Group 1 - Address-Family IPv4

State is ACTIVE

State duration 6 mins 55.006 secs

VRRPv3 Advertisements: sent 4288 (errors 0) - rcvd 0

VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0

Group Discarded Packets: 3856

```
IP address Owner conflicts: 0
IP address configuration mismatch : 0
Advert Interval errors : 0
Adverts received in Init state: 0
Invalid group other reason: 0
```

Group State transition:

```
Init to active: 0
Init to standby: 2 (Last change Mon Jun 16 11:19:36.316 UTC)
Standby to active: 2 (Last change Mon Jun 16 11:19:39.926 UTC)
Active to standby: 0
Active to init: 1 (Last change Mon Jun 16 11:17:49.978 UTC)
Standby to init: 0
```

```
switch# show vrrp statistics interface vlan100
```

VRRP is enabled

Interface vlan100 - VRRPv2 Statistics

```
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

Interface vlan100 - VRRPv3 Statistics

```
Invalid group ID packets received : 0
Invalid version packets received : 0
Invalid checksum packets received : 0
```

```
VRRP Statistics for interface vlan100 - Group 1 - Address-Family IPv4
State is ACTIVE
State duration 6 mins 55.006 secs
VRRPv3 Advertisements: sent 4288 (errors 0) - rcvd 0
VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
Group Discarded Packets: 3856
 IP address Owner conflicts: 0
 IP address configuration mismatch : 0
 Advert Interval errors : 0
 Adverts received in Init state: 0
 Invalid group other reason: 0
Group State transition:
 Init to active: 0
 Init to standby: 2 (Last change Mon Jun 16 11:19:36.316 UTC)
 Standby to active: 2 (Last change Mon Jun 16 11:19:39.926 UTC)
 Active to standby: 0
 Active to init: 1 (Last change Mon Jun 16 11:17:49.978 UTC)
 Standby to init: 0
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                                                                                              |
|------------------|-----------------------------------------------------------------------------------------------------------|
| 10.14            | Replaced the <b>ipv4</b> parameter with the <b>ip</b> parameter. The <b>ipv4</b> parameter is deprecated. |
| 10.08            | Updated command output for inclusive language                                                             |
| 10.07 or earlier | --                                                                                                        |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## shutdown

```
shutdown
no shutdown
```

### Description

Enables standby VRRP groups on the interface to route the traffic sent to virtual router's MAC address. It is recommended to enable this mode on VLANs where mc-lags are configured.

Disabled by default.

The **no** form of this command disables standby VRRP groups on the interface to route the traffic sent to virtual router's MAC address.





---

Only supported on SVI interfaces.

---

## Examples

Enabling standby VRRP groups on interface VLAN 10 to route traffic sent to the router's MAC address:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# vrrp dual-active-forwarding
```

Disabling the ability of standby VRRP groups on interface VLAN 10 to route traffic sent to the router's MAC address:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no vrrp dual-active-forwarding
```



---

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

---

## Command History

| Release    | Modification        |
|------------|---------------------|
| 10.12.1000 | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## timers advertise

```
timers advertise <ADVERTISE-IN-MILLISECONDS>
no timers advertise
```

### Description

Sets the advertisement interval in ms (100-40950). The default value is 1000. Advertisement interval can be configured in multiples of 1,000 ms.

The **no** form of this command sets the advertisement interval in ms to the default value of 1000.



---

This release does not support sub-second timer for VRRPv3.

---

## Examples

Setting the advertisement interval in ms to 2000:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# timers advertise 2000
```

Setting the advertisement interval in ms to the default value of 1000:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# no timers advertise
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## track (VRRP group)

```
track <OBJECT-ID>
no track <OBJECT-ID>
```

### Description

Sets the track object ID (1-128) for the group. The track object is first configured globally for the interface and then attached to the VRRP virtual router.



The track object must not track the same interface for which a VRRP group is configured.

The **no** form of this command removes the track object ID from the group.

### Examples

Setting the track object ID for the group:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# track 1
```

Removing the track object ID from the group:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# no track 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## track (VRRP virtual router)

```
track <OBJECT-ID>
no track <OBJECT-ID>
```

### Description

Configures a track object that can be associated with an interface. A change in interface state will then affect the priority of a VRRP group. By default, no interface is associated to a track object, so state is down.

The **no** form of this command deletes a tracked object for an interface. If it is not associated with a VRRP virtual router, a track object cannot be deleted.



Track cannot be configured by using port with no routing.

| Parameter   | Description                                         |
|-------------|-----------------------------------------------------|
| <OBJECT-ID> | Specify the track object ID value. Range: 1 to 128. |

### Examples

Configuring a tracked object:

```
switch(config)# track 1
```

Deleting a tracked object:

```
switch(config)# no track 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## track by

```
track by <OBJECT-ID>
no track by <OBJECT-ID>
```

### Description

Specifies an interface to be tracked when changes in the state of the interface affect the priority of a VRRP group. Once track is associated with an interface, the track state reflects the interface forwarding state.

The **no** form of this command removes an interface from tracking, affecting VRRP states of any interfaces associated with VRRP groups.



The VLAN interface 1 is always tracked.

| Parameter   | Description                                           |
|-------------|-------------------------------------------------------|
| <OBJECT-ID> | Specifies the track object ID value. Range: 1 to 128. |

### Example

Specifying an interface to be tracked:

```
switch (config)# interface 1/1/1
switch (config-if)# track by 1
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## version

version <VERSION-NUMBER>

### Description

Sets the protocol version for the VRRP group. Version change is allowed only for the IPv4 address-family. The default value is 2, which supports IPv4 with minimum 1 second advertisement interval. Value 3 supports IPv4 and IPv6 with minimum 1 second advertisement interval.

| Parameter        | Description                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <VERSION-NUMBER> | Specifies the VRRP protocol version. Possible values: 2 or 3. The default value is 2, which supports IPv4 with a minimum 1 second advertisement interval. |

### Example

Setting the protocol version for the VRRP group to 3:

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)# version 3
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## vrrp

```
vrrp <VRID> address-family {ip | ipv6}
no vrrp <VRID> address-family {ip | ipv6}
```

## Description

Creates a VRRP group and establishes VRRP group configuration context.

- A maximum of 16 VRRP groups, including both IPv4 and IPv6, are supported on an interface.
- A maximum of 256 VRRP groups is supported on a router. The groups can be IPv4 or IPv6 on a first come first serve basis.

The **no** form of this command deletes a VRRP group.

| Parameter                 | Description                                        |
|---------------------------|----------------------------------------------------|
| <VRID>                    | Selects the VRRP router ID value. Range: 1 to 255. |
| address-family [IP  IPv6] | Specifies which address family to use, IP or IPv6. |

## Examples

```
switch(config)# interface 1/1/1
switch(config-if)# vrrp 1 address-family ip
switch(config-if-vrrp)#

switch(config-if-vrrp)# no vrrp 1 address-family ip
```



For more information on features that use this command, refer to the IP Routing Guide for your switch model.

## Command History

| Release          | Modification                                                                                              |
|------------------|-----------------------------------------------------------------------------------------------------------|
| 10.14            | Replaced the <b>ipv4</b> parameter with the <b>ip</b> parameter. The <b>ipv4</b> parameter is deprecated. |
| 10.07 or earlier | --                                                                                                        |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## vrrp dual-active-forwarding

```
vrrp dual-active-forwarding
no vrrp dual-active-forwarding
```

### Description

Allows standby VRRP groups on an interface to route traffic sent to a virtual router's MAC address.

It is recommended to enable VRRP dual active forwarding on VLANs configured on MCLAG interfaces.

Disabled by default.

The **no** form of this command prevents standby VRRP groups on the interface to route traffic sent to the virtual router's MAC address.



---

VRRP dual active forwarding is only supported on SVI interfaces.

---



---

VRRP dual active forwarding and VRRP owner mode are mutually exclusive.

---

To verify the configuration of **vrrp dual-active-forwarding** use the [show vrrp](#) command.

## Examples

Enabling VRRP dual active forwarding on interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# vrrp dual-active-forwarding
```

Disabling VRRP dual active forwarding on interface VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no vrrp dual-active-forwarding
```



---

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

---

## Command History

| Release    | Modification        |
|------------|---------------------|
| 10.12.1000 | Command introduced. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Administrators or local user group members with execution rights for this command. |

### active-gateway

```
active-gateway
 ip [<IP-ADDRESS>] [mac <MAC-ADDRESS>]
 ipv6 [<IPv6-ADDRESS>] [[mac <MAC-ADDRESS>]
 l3-src-mac
 no ...
```

#### Description

Configures a virtual IP and virtual MAC for an interface VLAN. The `extended-mac` option stores MAC addresses in a supplemental table which allows configuring more than 16 virtual MAC addresses. The **no** form of this command removes the active gateway for active-active routing.



This configuration will disable flow tracking statistics collection.

| Parameter    | Description                                                                      |
|--------------|----------------------------------------------------------------------------------|
| ip           | Specifies the configuration of an IPv4 address.                                  |
| <IP-ADDRESS> | Specifies the IPv4 address. Syntax: <b>A.B.C..</b>                               |
| <MAC-ADDR>   | Specifies the Virtual MAC address. Syntax: xx:xx:xx:xx:xx:xx                     |
| ipv6         | Specifies the configuration of an IPv6 address.                                  |
| <IP-ADDRESS> | Specifies the IPv6 address. Syntax: <b>A:B::C:D</b>                              |
| <MAC-ADDR>   | Specifies the Virtual MAC address. Syntax: xx:xx:xx:xx:xx:xx                     |
| l3-src-mac   | Configures the virtual gateway MAC address as the source MAC for routed packets. |
| no           | Negates any configured parameter.                                                |

#### Usage

Before configuring active gateway, confirm that an IP address is on the SVI that is in the same subnet as the active gateway IP you are trying to configure. If an active gateway IP does not have an SVI IP with the same subnet, the CLI allows the configuration, but the active gateway IP will not be programmed in the kernel, resulting the active gateway to be unreachable.

It is highly recommended that you use an IPv6 link-local address as a gateway (VIP) on the active gateway IPv6 configuration.



If VRRP or active forwarding is configured on an SVI, active gateway cannot be configured. Active gateway with overlapping networks is not allowed. Maximum of 16 unique virtual MACs are supported in a system.

The maximum number of supported active gateways per switch is 4,000. Since a maximum of 31 secondary IPv4 addresses can be configured on an SVI, 32 IPv4 active gateways (along with the primary IPv4 address) can be configured per SVI with IP multinetting support. This support is also the same for IPv6 addresses.

If the active gateway is configured with the same IP as an SVI IP, then IPv6 DAD cannot be configured and the SVI IP cannot be changed.

The recommended order for configuring an active gateway with the same IPv6 address same as an SVI on both VSX Peers is:

1. IPv6 active gateway configuration
2. SVI IPv6 address configuration

If the configuration is applied in a different order, it may result in a DAD status of DUPLICATE. To remove the DUPLICATE status of the SVI IP address, perform a `shutdown` and `no shutdown` on the interface.



---

Do not use peer system MAC address as an active-gateway VMAC. If same MAC address is used, the VSX synchronization will try to sync the configuration on secondary switch and cause traffic disruptions.

---

## Examples

Configuring active-gateway, when the IP address is different from the SVI IP address on both VSX peers (valid for IPv4 and IPv6):

Switch 1:

```
switch1(config-if-vlan) # ip address 192.168.1.250/24
switch1(config-if-vlan) # active-gateway ip 192.168.1.253 mac 00:00:00:00:00:01
switch1(config-if-vlan) # active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
```

Switch 2:

```
switch2(config-if-vlan) # ip address 192.168.1.251/24
switch2(config-if-vlan) # active-gateway ip 192.168.1.253 mac 00:00:00:00:00:01
switch2(config-if-vlan) # active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
```

Configuring active-gateway when the IP address is the same as the SVI IP address on both VSX peers (valid for IPv4 and IPv6):

Switch 1:

```
switch1(config-if-vlan) # ip address 192.168.1.250/24
switch1(config-if-vlan) # active-gateway ip 192.168.1.250 mac 00:00:00:00:00:01
switch1(config-if-vlan) # active-gateway ipv6 fe80::100 mac 00:00:00:00:00:01
switch1(config-if-vlan) # ipv6 address link-local fe80::100/64
```

Switch 2:

```
switch2(config-if-vlan) # ip address 192.168.1.250/24
switch2(config-if-vlan) # active-gateway ip 192.168.1.250 mac 00:00:00:00:00:01
switch2(config-if-vlan) # active-gateway ipv6 fe80::100 mac 00:00:00:00:00:01
switch2(config-if-vlan) # ipv6 address link-local fe80::100/64
```

Configuring only the active gateway address:

```
switch(config-if-vlan) # ip address 192.168.1.250/24
switch(config-if-vlan) # active-gateway ip 192.168.1.250
```

Configuring only the active gateway IP MAC address:

```
switch2(config-if-vlan) # ip address 192.168.1.250/24
switch2(config-if-vlan) # active-gateway ip mac 00:00:00:01:00:01
```

Removing the active gateway for active-active routing (IPv6 and IPv4):

```
switch(config-if-vlan) # no active-gateway ip
switch(config-if-vlan) # no active-gateway ipv6
```

Removing the active gateway for active-active routing for an IP address:

```
switch(config-if-vlan) # no active-gateway ip 192.168.1.250
```

Removing the active gateway for active-active routing for virtual MAC addresses:

```
switch(config-if-vlan) # no active-gateway ip mac
```

When configuring the virtual active gateway for IPv6 on an SVI, it is recommended to use the same global IPv6 and active gateway IPv6 address. Similarly, if you want to use the IPv6 link-local address for the virtual active gateway then the same address should be configured for both the SVI and the active gateway.

Global IPv6 address:

```
switch(config-if-vlan) # ipv6 address 1001::1/64
switch(config-if-vlan) # active-gateway ipv6 1001::1
switch(config-if-vlan) # active-gateway ipv6 mac 00:00:00:00:aa:01
```

IPv6-Link-Local address:

```
switch(config-if-vlan) # ipv6 address link-local fe80::1/64
switch(config-if-vlan) # active-gateway ipv6 fe80::1
switch(config-if-vlan) # active-gateway ipv6 mac 00:00:00:00:aa:01
```

Configuring l3-src-mac, when only a IPv4 virtual MAC is configured, a IPv4 virtual MAC is used as a source MAC for IPv4 routed packets.

```
switch(config-if-vlan)# ip address 192.168.1.250/24
switch(config-if-vlan)# active-gateway ip 192.168.1.253 mac 00:00:00:00:00:01
switch(config-if-vlan)# active-gateway l3-src-mac
```

Configuring l3-src-mac, when only a IPv6 virtual MAC is configured, a IPv6 virtual MAC is used as a source MAC for IPv6 routed packets.

```
switch(config-if-vlan)# ip address 192.168.1.250/24
switch(config-if-vlan)# active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
switch(config-if-vlan)# active-gateway l3-src-mac
```

Configuring l3-src-mac, when both IPv4 and IPv6 virtual MACs are configured, IPv4 virtual MAC is used as source MAC for IPv4 and IPv6 routed packets. It is recommended to use the same virtual MAC when both ipv4 and ipv6 virtual MACs are configured.

```
switch(config-if-vlan)# ip address 192.168.1.250/24
switch(config-if-vlan)# active-gateway ip 192.168.1.253 mac 00:00:00:00:00:01
switch(config-if-vlan)# active-gateway ipv6 fe80::01 mac 00:00:00:00:00:01
switch(config-if-vlan)# active-gateway l3-src-mac
```



When ipv4 and ipv6 virtual MACs are same, 8325 and 10000 switches support 512 SVIs. When ipv4 and ipv6 virtual MACs are different, 8325 and 10000 switches support 341 SVIs.

## Configuration table for supported SVIs

| Configuration                                                                         | Platforms                               | Supported SVIs |
|---------------------------------------------------------------------------------------|-----------------------------------------|----------------|
| When the l3-src-mac IPv4 is configured on SVI along with the active-gateway           | 8320                                    | Up to 190      |
|                                                                                       | 8325 and 10000                          | Up to 380      |
|                                                                                       | 8360 and 6400                           | Up to 384      |
|                                                                                       | 8100                                    | Up to 256      |
| When the l3-src-mac IPv4 and IPv6 are configured on SVI along with the active-gateway | 8320                                    | Up to 165      |
|                                                                                       | 8325 and 10000                          | Up to 330      |
|                                                                                       | 8360 and 6400                           | Up to 384      |
|                                                                                       | 8100                                    | Up to 256      |
| When the VSX active-forwarding, VRRP and virtual-mac features are configured          | 8320, 8325, 8360, 8100, 6400, and 10000 | Goes down      |

Configuring l3-src-mac, when no virtual MACs are configured, the System MAC is used as source MAC for routed packets. Such configuration can generate a CLI warning as shown.

```
switch(config-if-vlan)# ip address 192.168.1.250/24
switch(config-if-vlan)# active-gateway l3-src-mac
Warning: Active Gateway VMAC is not configured
```

With VSX-Sync configured, "active-gateway l3-src-mac" configuration syncs to the peer device. Following configuration from vsx-primary device can get synced to vsx-secondary device.

VSX-Primary-Switch:

```
vsx-pri-switch(config-if-vlan)# ip address 192.168.1.250/24
vsx-pri-switch(config-if-vlan)# active-gateway ip 192.168.1.253 mac
00:00:00:00:00:01
vsx-pri-switch(config-if-vlan)# active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
vsx-pri-switch(config-if-vlan)# active-gateway l3-src-mac
```

For VSX-peer devices, without VSX-Sync configured, it is expected that virtual MACs and l3-src-mac configurations are identical on both devices for a given interface VLAN. If configurations don't match, each device may end up using different source MAC for routed traffic for this interface and connectivity from connected devices to this VSX-peer devices may get affected.

VSX-Primary-Switch:

```
vsx-pri-switch(config-if-vlan)# ip address 192.168.1.250/24
vsx-pri-switch(config-if-vlan)# active-gateway ip 192.168.1.253 mac
00:00:00:00:00:01
vsx-pri-switch(config-if-vlan)# active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
vsx-pri-switch(config-if-vlan)# active-gateway l3-src-mac
```

VSX-Secondary-Switch:

```
vsx-sec-switch(config-if-vlan)# ip address 192.168.1.250/24
vsx-sec-switch(config-if-vlan)#
vsx-sec-switch(config-if-vlan)# active-gateway ip 192.168.1.253 mac
00:00:00:00:00:01
vsx-sec-switch(config-if-vlan)# active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
vsx-sec-switch(config-if-vlan)# active-gateway l3-src-mac
```

When l3-src-mac option is unconfigured, System MAC uses as source MAC for routed traffic.

```
switch(config-if-vlan)# no active-gateway l3-src-mac
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release | Modification                                                                 |
|---------|------------------------------------------------------------------------------|
| 10.14   | Added information related to role based IPFIX.                               |
| 10.10   | Added the <b>l3-src-mac</b> parameter and command supported for 9300 switch. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Administrators or local user group members with execution rights for this command. |

## config-sync disable

```
config-sync disable
no config-sync disable
```

### Description

Pauses VSX synchronization.

The **no** form of this command restarts VSX synchronization.

### Examples

Pauses VSX configuration synchronization:

```
switch(config)# vsx
switch(config-vsx)# config-sync disable
```

Enables the VSX configuration synchronization:

```
switch(config)# vsx
switch(config-vsx)# no config-sync disable
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## inter-switch-link {<PORT-NUM> | lag <LAG-ID>}

```
inter-switch-link {<PORT-NUM> | lag <LAG-ID>}
no inter-switch-link [lag <LAG-ID>]
```

### Description

Configures a physical port or a LAG as an interswitch link port. Only one port or LAG can be configured to act as an ISL. Once a port is configured as an ISL, it becomes a part of all VLANs in a system.

The **no** form of this command clears the configuration of the interswitch link port from a physical port or a LAG.

| Parameter                     | Description                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;PORT-NUM&gt;</code> | Specifies a physical port on the switch. Use the format <code>member/slot/port</code> (for example, <code>1/3/1</code> ). Sets the port to act as ISL |
| <code>&lt;LAG-ID&gt;</code>   | Specifies the LAG ID. Run the <code>show capacities</code> command for the maximum number of VSX LAGs supported for your particular type of switch.   |

## Examples

Configuring port 1/1/1 as an interswitch link port:

```
switch(config-vsx) # inter-switch-link 1/1/1
```

Configuring LAG 100 as an interswitch link port:

```
switch(config-vsx) # inter-switch-link lag 100
```

Clears the interswitch link port:

```
switch(config-vsx) # no inter-switch-link
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification                                                                          |
|------------------|---------------------------------------------------------------------------------------|
| 10.08            | Added optional <code>lag</code> parameter to the <code>no</code> form of the command. |
| 10.07 or earlier | --                                                                                    |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-vsx</code> | Administrators or local user group members with execution rights for this command. |

## inter-switch-link dead-interval

```
inter-switch-link dead-interval <DEAD-INTERVAL>
```

```
no inter-switch-link dead-interval
```

## Description

Sets the dead interval for the interswitch link protocol. The dead interval is the amount of time to wait for hellos from a peer before declaring the peer to be dead. The default dead interval time is 20 seconds.

The **no** form of this command resets the interswitch link dead interval to the default of 20 seconds.

| Parameter                          | Description                                                               |
|------------------------------------|---------------------------------------------------------------------------|
| <code>&lt;DEAD-INTERVAL&gt;</code> | Specifies the dead interval in seconds. Required. Range: 2 to 20 seconds. |

## Examples

Setting the dead interval for the interswitch link protocol to 10 seconds:

```
switch(config)# vsx
switch(config-vsx)# inter-switch-link dead-interval 10
```

Setting the dead interval for the interswitch link protocol to the default:

```
switch(config)# vsx
switch(config-vsx)# no vsx inter-switch-link dead-interval
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## inter-switch-link hello-interval

```
inter-switch-link hello-interval <HELLO-INTERVAL>
no inter-switch-link hello-interval
```

## Description

Configures the interswitch link hello-interval. The hello interval determines the frequency of a hello packet exchange to confirm the control plane of the peer is alive. The default hello-interval is 1 second.

The **no** form of this command sets the interswitch link hello-interval to the default of 1 second.

| Parameter                           | Description                                                 |
|-------------------------------------|-------------------------------------------------------------|
| <code>&lt;HELLO-INTERVAL&gt;</code> | Specifies hello interval in seconds. Range: 1 to 5 seconds. |

## Examples

Configuring the interswitch link hello-interval to 3 seconds:

```
switch(config)# vsx
switch(config-vsx)# inter-switch-link hello-interval 3
```

Resetting the interswitch link hello-interval to the default of 1 second:

```
switch(config)# vsx
switch(config-vsx)# no inter-switch-link hello-interval
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# inter-switch-link hold-time

```
inter-switch-link hold-time <HOLD-INTERVAL>
no inter-switch-link hold-time
```

## Description

Sets the holdtime for the interswitch link protocol. A port is treated as down only when it stays down for the configured holdtime interval. The default holdtime is 0 seconds.

The **no** form of this command sets the interswitch link protocol holdtime to the default of 0 seconds.

| Parameter                          | Description                                                              |
|------------------------------------|--------------------------------------------------------------------------|
| <code>&lt;HOLD-INTERVAL&gt;</code> | Specifies the hold interval in seconds. Required. Range: 0 to 3 seconds. |

## Examples

Setting the holdtime for interswitch link protocol to 2 seconds:



```
switch(config)# vsx
switch(config-vsx)# inter-switch-link hold-time 2
```

Setting the interswitch link protocol holdtime to the default of 0 seconds:

```
switch(config)# vsx
switch(config-vsx)# no inter-switch-link hold-time
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## inter-switch-link peer-detect-interval

```
inter-switch-link peer-detect-interval <PEER-DETECT-INTERVAL>
no inter-switch-link peer-detect-interval
```

### Description

Sets the amount of time in seconds that the VSX switch waits for the ISL interface to link up after a reboot. If the ISL link does not come up within this time window, the VSX switch declares itself as split from its peer. The default peer detect interval is 300 seconds.

The **no** form of this command sets the interswitch link protocol peer detect interval to the default of 300 seconds.

| Parameter              | Description                                                                         |
|------------------------|-------------------------------------------------------------------------------------|
| <PEER-DETECT-INTERVAL> | Specifies the peer detect interval in seconds. Required. Range: 60 to 1800 seconds. |

### Usage

After a VSX switch reboots, the switch waits 5 minutes by default to receive a hello packet before it declares itself to be out-of-sync. The **inter-switch-link peer-detect-interval <PEER-DETECT-INTERVAL>** command lets you change how long the switch waits to receive the hello packet before the switch declares itself to be out-of-sync.

### Examples

Setting the peer detect interval to 180 seconds:

```
switch(config)# vsx
switch(config-vsx)# inter-switch-link peer-detect-interval 180
```

Restoring the peer detect interval to the default (300 seconds):

```
switch(config)# vsx
switch(config-vsx)# no inter-switch-link peer-detect-interval
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## interface lag multi-chassis

```
interface lag <LAG-ID> multi-chassis [static]
no interface lag <LAG-ID>
```

### Description

Configures a given LAG as a dynamic multichassis LAG (VSX LAG), which supports a maximum of four member links per switch segment. A VSX LAG across a downstream switch can have at most a total of eight member links.

The **no** form of this command removes a VSX LAG.

| Parameter | Description                                                                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LAG-ID>  | Specifies the LAG ID. Run the <code>show capacities vsx</code> command for the maximum number of VSX LAGs supported for your particular type of switch; however, the maximum VSX LAG value considers that one port is used for the ISL, which is not a VSX LAG. Required. |
| static    | Specifies the multichassis LAG as static. Optional.                                                                                                                                                                                                                       |

### Usage

A VSX LAG across a VSX pair can have at most a total of 16 interfaces.



- When creating a VSX LAG, select an equal number of member links in each segment for load balancing, such as four member links (one segment) and four member links (another segment). Do not create a VSX LAG with four member links in one switch and two member links on another segment. A switch can have a maximum of four member links.
- Make sure that the VSX LAG interface on both the VSX primary and secondary switches has a member port configured and enabled.
- Make sure that you also have a non-VSX port that is available for the ISL.
- It is recommended to use hashing algorithm value as **I3-src-dst** (default) or **I2-src-dst** on the VSX LAG.

You cannot change the mode of a multichassis LAG without removing the multichassis LAG first. To change a pre-existing VSX LAG to a static VSX LAG, first remove the VSX LAG with the **no interface lag <LAG-ID>** command. Then, enter the **interface lag <LAG-ID> multi-chassis static** command.

## Examples

Configuring LAG 100 as a VSX LAG:

```
switch(config)# interface lag 100 multi-chassis
```

Removing LAG 100 as a VSX LAG:

```
switch(config)# no interface lag 100
```

Specifying LAG 100 as a static VSX LAG:

```
switch(config)# interface lag 100 multi-chassis static
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## ip icmp redirect

```
ip icmp redirect
no ip icmp redirect
```

## Description

Enables the sending of ICMPv4 and ICMPv6 redirect messages to the source host. Enabled by default. The **no** form of this command disables ICMPv4 and ICMPv6 redirect messages to the source host.

## Examples

Enabling ICMP redirect messages:

```
switch(config)# ip icmp redirect
```

Disabling ICMP redirect messages:

```
switch(config)# no ip icmp redirect
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

# keepalive dead-interval

```
keepalive dead-interval <DEAD-INTERVAL>
no keepalive dead-interval
```

## Description

Sets the dead-interval for keepalive protocol. The dead interval is the amount of time to wait for hellos from a peer before declaring the peer to be dead. The default dead-interval is 3 seconds.

The **no** form of this command sets the interswitch link dead-interval to the default of 3 seconds.

| Parameter                     | Description                                                    |
|-------------------------------|----------------------------------------------------------------|
| dead-interval <DEAD-INTERVAL> | Specifies the dead-interval in seconds. Range: 2 to 20 seconds |

## Examples

Setting the dead-interval for keepalive protocol to 10 seconds:

```
switch(config)# vsx
switch(config-vsx)# keepalive dead-interval 10
```

Setting the dead-interval for keepalive protocol to the default:

```
switch(config)# vsx
switch(config-vsx)# no keepalive dead-interval
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# keepalive hello-interval

```
keepalive hello-interval <HELLO-INTERVAL>
no keepalive hello-interval
```

## Description

Sets the hello-interval for keepalive protocol. The hello interval determines the frequency of a hello packet exchange to confirm the peer is alive. The default hello-interval is 1 second.

The **no** form of this command sets the hello-interval for keepalive protocol to the default of 1 second.

| Parameter                       | Description                                                    |
|---------------------------------|----------------------------------------------------------------|
| hello-interval <HELLO-INTERVAL> | Specifies the hello-interval in seconds. Range: 1 to 5 seconds |

## Examples

Setting the hello-interval for keepalive protocol to 3 seconds:

```
switch(config)# vsx
switch(config-vsx)# keepalive hello-interval 3
```

Resetting the hello-interval for keepalive protocol to the default:

```
switch(config)# vsx
switch(config-vsx)# no keepalive hello-interval
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## keepalive peer

```
keepalive peer <PEER-IP-ADDR> source <SOURCE-IP-ADDR> [vrf <VRF-NAME>]
no keepalive [peer <PEER-IP-ADDR> source <SOURCE-IP-ADDR> [vrf <VRF-NAME>]]
```

## Description

Sets the source and peer IP addresses for keepalive packets in a specified VRF. If a VRF is not specified, it sets to the default VRF. Both IPv4 and IPv6 are supported. Source and peer IP addresses for keepalive packets can also be configured on the management VRF.

The **no** form of this command removes the source and peer IP addresses and VRF for the keepalive protocol. VSX continues to work.

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer <PEER-IP-ADDR> | Specifies the peer IPv4 or IPv6 address. Syntax: A.B.C.D                                                                                                                                                                                                                                                                                                       |
| source <IP-ADDR>    | Specifies the source IPv4 or IPv6 address. The source IP address is the IP address assigned to the keepalive interface on the switch. For example, if you are entering this command on the primary switch, the source IP address would be the IP address assigned to the keepalive interface on the primary switch. Syntax: A.B.C.D                            |
| vrf <VRF-NAME>      | Specifies the VRF name. If you are entering this command on the primary switch, the peer IP address is the IP address assigned to the keepalive interface for the secondary switch. If you are entering this command on the secondary switch, the peer IP address is the IP address assigned to the keepalive interface for the primary switch. Syntax: String |

## Usage

To configure the keepalive feature, enter this command once on the primary switch and once on the secondary switch. The keepalive feature is recommended for redundancy. If the ISL link goes down, the keepalive connection keeps the traffic moving so that the peer and secondary switches can continue to

communicate. The keepalive connection is established over a routed network, and it does not have to be a dedicated peer-to-peer link unlike ISL.

## Examples

Setting the source and peer IP addresses for keepalive in the default VRF:

```
switch(config)# vsx
switch(config-vsx)# keepalive peer 192.168.1.1 source 192.168.1.5
```

Setting the source and peer IPv6 addresses for keepalive in the default VRF:

```
switch(config)# vsx
switch(config-vsx)# keepalive peer 2002:2 source 2002::3
```

Setting the source and peer IP addresses for keepalive in the vrf1:

```
switch(config)# vsx
switch(config-vsx)# keepalive peer 10.0.0.1 source 10.0.0.2 vrf vrf1
```

Setting the source and peer IP addresses for keepalive in the management VRF:

```
switch(config)# vsx
switch(config-vsx)# keepalive peer 10.0.0.1 source 10.0.0.2 vrf mgmt
```

Removing the source and peer IP addresses and VRF for the keepalive protocol:

```
switch(config)# vsx
switch(config-vsx)# no keepalive
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.08            | Added optional parameters to the <b>no</b> form of the command. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## keepalive udp-port

```
keepalive udp-port <PORT-NUM>
no keepalive udp-port
```

## Description

Sets the UDP port for the keepalive protocol.

The **no** form of this command sets the UDP port for keepalive protocol to the default of 7678.

| Parameter           | Description                                  |
|---------------------|----------------------------------------------|
| udp-port <PORT-NUM> | Specifies UDP port number. Range: 1024-65535 |

## Examples

Setting the UDP port for keepalive protocol to 2000:

```
switch(config)# vsx
switch(config-vsx)# keepalive udp-port 2000
```

Setting the UDP port for keepalive protocol to the default of 7678:

```
switch(config)# vsx
switch(config-vsx)# no keepalive udp-port
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## lacp fallback

```
lacp fallback
no lacp fallback
```

## Description

Sets LACP fallback on a VSX LAG port. When no LACP partner is detected, the VSX LAG port makes members of the VSX LAG function as nonbonded interfaces. To create a VSX LAG, use the **interface lag multi-chassis** command.

The **no** form of this command sets the VSX LAG to a block state when no LACP partner is detected.



## Usage

LACP fallback is supported only when there is a single link from the downstream or peer device to each VSX node.



---

Even though this command appears to be accepted on a standard/non-VSX LAG, the fallback feature works only on a VSX LAG (multichassis LAG) interface.

---

## Examples

Enabling LACP fallback:

```
switch(config)# interface lag 1
switch(config-lag-if)# lacp fallback
```

Disables LACP fallback:

```
switch(config)# interface lag 1
switch(config-lag-if)# no lacp fallback
```



---

For more information on features that use this command, refer to the VSX Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-lag-if   | Administrators or local user group members with execution rights for this command. |

## linkup-delay-timer

```
linkup-delay-timer <DELAY-TIMER>
no linkup-delay-timer [<DELAY-TIMER>]
```

### Description

Configures the VSX link-up delay timer. The VSX delay timer feature lets you configure the delay timer, which delays bringing downstream VSX links up, following a VSX device reboot or an ISL flap.

The **no** form of this command restores the VSX link-up delay timer to a default of 180 seconds.

| Parameter                        | Description                                                              |
|----------------------------------|--------------------------------------------------------------------------|
| <code>&lt;DELAY-TIMER&gt;</code> | Specifies the VSX LAG bring-up delay in seconds. Range: 0 to 600 seconds |

## Usage

The recommended delay timer setting is determined by the number of MAC addresses, ARPv4, and routes. The link-up delay timer might need to be set to a higher value for larger networks, depending on the ARP and routing table size.

## Examples

Setting the VSX link-up delay timer to 35 seconds:

```
switch(config)# vsx
switch(config-vsx)# linkup-delay-timer 35
```

Setting the VSX link-up delay timer to the default:

```
switch(config)# vsx
switch(config-vsx)# no linkup-delay-timer
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification                                                                                    |
|------------------|-------------------------------------------------------------------------------------------------|
| 10.08            | Added optional <code>&lt;DELAY-TIMER&gt;</code> parameter to the <b>no</b> form of the command. |
| 10.07 or earlier | --                                                                                              |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-vsx</code> | Administrators or local user group members with execution rights for this command. |

## linkup-delay-timer exclude lag-list

```
linkup-delay-timer exclude lag-list <LAG-LIST>
no linkup-delay-timer exclude lag-list <LAG-LIST>
```

## Description

Configures the VSX link-up delay timer exclude list. It excludes the bringing up of specified downstream VSX LAGs, following a device reboot or an ISL flap.

The **no** form of this command unconfigures the VSX link-up delay timer exclude list.

| Parameter                     | Description                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;LAG-LIST&gt;</code> | Specifies a range or a set of LAG interfaces to exclude. For example: 1 or 1-10 or 1, 2, 3 or 1, 2-10. Range: 1-128 characters. |

## Examples

Specifying LAGs to exclude LAG 100:

```
switch(config)# vsx
switch(config-vsx)# linkup-delay-timer exclude lag-list 100
```

Unconfiguring the VSX link-up delay timer exclude list for LAG 100:

```
switch(config)# vsx
switch(config-vsx)# no linkup-delay-timer exclude lag-list 100
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# neighbor <IP-ADDRESS> vsx-sync-exclude

neighbor <IP-ADDRESS> vsx-sync-exclude

## Description

Excludes the neighbor configurations from VSX sync operations at run time.

When VSX sync is configured for BGP, the VSX secondary peer cannot have any configuration of its own. If the VSX primary has a configuration, that will always get synchronized to the VSX secondary. Any modification done in the synchronized configurations on the VSX secondary will be overwritten by the VSX primary configuration after a VSX config sync. If there is a new configuration on the VSX secondary, then that configuration also gets deleted after a VSX config sync.

On the VSX primary, a configuration with vsx-sync-exclude enabled excludes the neighbor configurations from synchronizing to the VSX -secondary, allowing the VSX secondary can have it own entry for the corresponding neighbor configurations.

On the VSX secondary, a configuration with `vsx-sync-exclude` enabled excludes the neighbor configurations being deleted or overwritten by the VSX primary configuration during a VSX configuration sync.

---

VSX -sync for BGP has to be configured at the VSX context for this command to take effect.

---



To maintain uniqueness of a switch in the autonomous system, the **bgp router-id**, **bgp cluster-id** and **bgp neighbor update-source** values are not synchronized. This exclusion is required for BGP functionality to work seamlessly in a VSX topology.

---

## Examples

Excluding VSX sync for the BGP neighbor:

```
switch(config-bgp) # neighbor 1.1.1.1 vsx-sync-exclude
```



---

For more information on features that use this command, refer to the VSX Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-bgp      | Administrators or local user group members with execution rights for this command. |

## role {primary | secondary}

```
role {primary | secondary}
no role
```

### Description

Configures the VSX device role.

The **no** form of this command removes the device role of the switch in VSX and causes the interswitch link to be out-of-sync.

| Parameter             | Description                                                         |
|-----------------------|---------------------------------------------------------------------|
| {primary   secondary} | Selects the VSX role to either primary or secondary for the device. |

### Usage

VSX has no default role defined for the device. The device role assigns the device as the primary or secondary for VSX synchronization. For ISL to be in-sync, one device in VSX must be configured as the primary and the other device must be configured as the secondary.

## Examples

Setting the VSX role to primary:

```
switch(config)# vsx
switch(config-vsx)# role primary
```

Removing the device role:

```
switch(config)# vsx
switch(config-vsx)# no role
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## show active-gateway

```
show active-gateway [vsx-peer]
```

### Description

Displays the gateway information configured on SVIs, such as:

- Number of active-gateway interface VLANs
- Number of IPv4 active-gateway interface VLANs
- Number of IPv6 active-gateway interface VLANs
- Per virtual MAC address
  - IPv4 reference count and its interface VLANs
  - IPv6 reference count and its interface VLANs

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

```

primary# show active-gateway
Number of active-gateway interface VLANs : 265
Number of IPv4 active-gateway interface VLANs : 264
Number of IPv6 active-gateway interface VLANs : 1
VMAC 00:00:00:01:01:16 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan192-223
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:11 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan32-63
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:17 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan224-255
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:18 :
 IPv4 ref count : 6
 IPv4 interface VLANs : vlan256-259,300-301
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:13 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan96-127
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:12 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan64-95
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:20 :
 IPv4 ref count : 1
 IPv4 interface VLANs : vlan4040
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:14 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan128-159
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:10 :
 IPv4 ref count : 31
 IPv4 interface VLANs : vlan1-31
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:01:01:15 :
 IPv4 ref count : 32
 IPv4 interface VLANs : vlan160-191
 IPv6 ref count : 0
 IPv6 interface VLANs : none
VMAC 00:00:00:03:00:12 :
 IPv4 ref count : 1
 IPv4 interface VLANs : vlan2000
 IPv6 ref count : 1
 IPv6 interface VLANs : vlan4000
VMAC 00:00:00:01:01:19 :
 IPv4 ref count : 1
 IPv4 interface VLANs : vlan4000

```

```
IPv6 ref count : 0
IPv6 interface VLANs : none
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show active-gateway <IFNAME>

```
show active-gateway <IFNAME> [vsx-peer]
```

### Description

Displays the gateway information per SVI, such as:

- Active-Gateway IPV4 and its MAC address
- Active-Gateway IPV6 and its MAC address

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IFNAME>  | Specifies the VSX interface name.                                                                                                                                                                                                |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

```
switch# show active-gateway vlan2000
Active-gateway IPv4 MAC address : 00:00:00:01:01:18
Active-gateway IPv4 address
 173.6.1.10
 173.7.1.10
Active-gateway IPv6 MAC address : 00:00:00:03:00:12
Active-gateway IPv6 address
 173::2
 173::3
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show interface <VLAN-NAME>

`show interface <VLAN-NAME> [vsx-peer]`

### Description

Displays a virtual IPv4/IPv6 and MAC configured for active-active routing.

| Parameter   | Description                                                                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <VLAN-NAME> | Specifies the VLAN name. Syntax: string                                                                                                                                                                                          |
| vsx-peer    | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

```
switch# show interface vlan100
```

```
Interface vlan100 is up
Admin state is up
Hardware: Ethernet, MAC Address: 48:0f:cf:af:c1:9e
IPv4 address 192.168.1.1/24
IPv4 address 192.168.2.1/24 secondary
 active-gateway ip mac 00:00:00:00:00:01
 active-gateway ip 192.168.1.1
 active-gateway ip 192.168.2.2
 active-gateway ipv6 mac 00:00:00:00:00:01
 active-gateway ipv6 fe80::1
```

| Statistics | RX  | TX | Total |
|------------|-----|----|-------|
| L3 Packets | 8   | 2  | 10    |
| L3 Bytes   | 812 | 80 | 892   |





For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show lacp aggregates

`show lacp aggregates [<LAG-NAME>] [vsx-peer]`

## Description

Displays a specified LAG or all configured LAGs along with VSX LAGs.

| Parameter  | Description                                                                                                                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LAG-NAME> | Specifies the LAG name. Optional. Syntax: string                                                                                                                                                                                 |
| vsx-peer   | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Displaying all configured LAGs along with VSX LAGs:

```
switch# show lacp aggregates

Aggregate name : lag100 (multi-chassis)
Interfaces : 1/1/44
Peer interfaces : 1/1/44
Heartbeat rate : Slow
Hash : 13-src-dst
Aggregate mode : Active
```

Displaying a specified LAG:

```
switch# show lacp aggregates lag100

Aggregate name : lag100 (multi-chassis)
Interfaces : 1/1/44
```

```
Peer interfaces : 1/1/44
Heartbeat rate : Slow
Hash : 13-src-dst
Aggregate mode : Active
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show lacp interfaces

```
show lacp interfaces [<IFNAME>] [vsx-peer]
```

## Description

Displays an LACP configuration of the physical interfaces, including VSXs. If an interface name is passed as argument, it only displays an LACP configuration of a specified interface.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IFNAME>  | Optional: Specifies an interface name.                                                                                                                                                                                           |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

This example displays an LACP configuration of the physical interfaces. One of the interfaces has the `lacp-block` forwarding state. If a VSX switch has loop protect enabled on an interface and a loop occurs, VSX blocks the interface to stop the loop. The forwarding state of the blocked interface is set to `lacp-block`.

```
switch# show lacp interfaces
State abbreviations :
A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
```

X - State m/c expired                      E - Default neighbor state

Actor details of all interfaces:

```

--
Intf Aggr Port Port State System-id System Aggr Forwarding
 name id Pri State Pri Pri Key State

--
1/1/1 lag10 17 1 ALFOE 70:72:cf:37:a3:5c 20 10 lacp-block
1/1/2 lag128 69 1 ALFNCD 70:72:cf:37:a3:5c 20 128 up
1/1/3 lag128 14 1 ALFNCD 70:72:cf:37:a3:5c 20 128 up
1/1/4 lag128 down
1/1/5 lag20 up
```

Partner details of all interfaces:

```

Intf Aggr Partner Port State System-id System Aggr
 name Port-id Pri State Priority Key

1/1/1 lag10 0 65534 PLFOEX 00:00:00:00:00:00 65534 0
1/1/2 lag128 69 1 PLFNCD 70:72:cf:8c:60:a7 65534 128
1/1/3 lag128 14 1 PLFNCD 70:72:cf:8c:60:a7 65534 128
1/1/4 lag128
1/1/5 lag20
```

Displaying static LAG:

```
switch# show lacp interfaces
State abbreviations :
A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state

Actor details of all interfaces:

Intf Aggr Port Port State System-id System Aggr Forwarding
 Name Id Pri State Pri Pri Key State

1/1/1 lag10 up
1/1/2 lag10 up

Partner details of all interfaces:

Intf Aggr Port Port State System-id System Aggr
 Name Id Pri State Pri Key

1/1/1 lag10
1/1/2 lag10
```

Displaying an LACP configuration of the 1/1/1 interface:

```
switch# show lacp interfaces 1/1/1

State abbreviations :
A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
```

X - State m/c expired                      E - Default neighbor state

Aggregate-name : lag1

|                 |  | Actor             | Partner           |
|-----------------|--|-------------------|-------------------|
| Port-id         |  | 28                | 31                |
| Port-priority   |  | 1                 | 1                 |
| Key             |  | 1                 | 1                 |
| State           |  | ALFNCD            | ALFNCD            |
| System-id       |  | 98:f2:b3:68:40:a0 | 98:f2:b3:68:60:a6 |
| System-priority |  | 65534             | 65534             |

Displaying an LACP configuration after loop-protect is enabled on the primary VSX switch:

```
switch# show lacp interfaces
```

State abbreviations :

A - Active                      P - Passive                      F - Aggregable I - Individual  
S - Short-timeout L - Long-timeout N - InSync                      O - OutofSync  
C - Collecting                      D - Distributing  
X - State m/c expired                      E - Default neighbor state

Actor details of all interfaces:

| Intf   | Aggr<br>Name | Port<br>Id | Port<br>Pri | State  | System-ID         | System<br>Pri | Aggr<br>Key | Forwarding<br>State |
|--------|--------------|------------|-------------|--------|-------------------|---------------|-------------|---------------------|
| 1/4/14 | lag1(mc)     | 206        | 1           | ALFNCD | f8:60:f0:06:49:00 | 65534         | 1           | up                  |
| 1/5/15 | lag2(mc)     |            |             |        |                   |               |             | down                |

Partner details of all interfaces:

| Intf   | Aggr<br>Name | Port<br>Id | Port<br>Pri | State  | System-ID         | System<br>Pri | Aggr<br>Key |
|--------|--------------|------------|-------------|--------|-------------------|---------------|-------------|
| 1/4/14 | lag1(mc)     | 130        | 1           | ALFNCD | f8:60:f0:06:87:00 | 65534         | 1           |
| 1/5/15 | lag2(mc)     |            |             |        |                   |               |             |

Displaying an LACP configuration after loop-protect is enabled on the secondary VSX switch:

```
switch# show lacp interfaces
```

State abbreviations :

A - Active                      P - Passive                      F - Aggregable I - Individual  
S - Short-timeout L - Long-timeout N - InSync                      O - OutofSync  
C - Collecting                      D - Distributing  
X - State m/c expired                      E - Default neighbor state

Actor details of all interfaces:

| Intf  | Aggr<br>Name | Port<br>Id | Port<br>Pri | State  | System-ID         | System<br>Pri | Aggr<br>Key | Forwarding<br>State |
|-------|--------------|------------|-------------|--------|-------------------|---------------|-------------|---------------------|
| 1/3/2 | lag1(mc)     | 1130       | 1           | ALFNCD | f8:60:f0:06:49:00 | 65534         | 1           | up                  |
| 1/9/3 | lag2(mc)     |            |             |        |                   |               |             | down                |

Partner details of all interfaces:

| Intf  | Aggr<br>Name | Port<br>Id | Port<br>Pri | State  | System-ID         | System<br>Pri | Aggr<br>Key |
|-------|--------------|------------|-------------|--------|-------------------|---------------|-------------|
| 1/3/2 | lag1 (mc)    | 131        | 1           | ALFNCD | f8:60:f0:06:87:00 | 65534         | 1           |
| 1/9/3 | lag2 (mc)    |            |             |        |                   |               |             |



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show lacp interfaces multi-chassis

show lacp interfaces multi-chassis [<IFNAME>] [vsx-peer]

## Description

Shows all configured VSX remote interface details. The interface that has the ALFNCD status has been synced with the partner and is ready for flow distribution.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IFNAME>  | Specifies the VSX interface name. Optional.                                                                                                                                                                                      |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

```
switch# show lacp interfaces multi-chassis

State abbreviations :
A - Active P - Passive F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync O - OutofSync
C - Collecting D - Distributing
X - State m/c expired E - Default neighbor state
```

Actor details of all interfaces:

| Intf  | Aggregate name | Port id | Port Priority | State  | System-ID         | System Priority | Aggr Key |
|-------|----------------|---------|---------------|--------|-------------------|-----------------|----------|
| 1/1/2 | lag100(mc)     | 2       | 1             | ALFNCD | 08:00:09:13:06:7c | 65534           | 100      |

Partner details of all interfaces:

| Intf  | Aggregate name | Partner Port-id | Port Priority | State  | System-ID         | System Priority | Aggr Key |
|-------|----------------|-----------------|---------------|--------|-------------------|-----------------|----------|
| 1/1/2 | lag100(mc)     | 2               | 1             | ALFNCD | 08:00:09:05:24:f6 | 65534           | 10       |

Remote Actor details of all interfaces:

| Intf  | Aggregate name | Port id | Port Priority | State  | System-ID         | System Priority | Aggr Key |
|-------|----------------|---------|---------------|--------|-------------------|-----------------|----------|
| 1/1/2 | lag100(mc)     | 1002    | 1             | ALFNCD | 08:00:09:13:06:7c | 65534           | 100      |

Remote Partner details of all interfaces:

| Intf  | Aggregate name | Partner Port-id | Port Priority | State  | System-ID         | System Priority | Aggr Key |
|-------|----------------|-----------------|---------------|--------|-------------------|-----------------|----------|
| 1/1/2 | lag100(mc)     | 3               | 1             | ALFNCD | 08:00:09:05:24:f6 | 65534           | 10       |



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show running-config interface

show running-config interface

### Description

Displays all configured interface commands, including VSX commands.

### Example

```
switch# show running-config interface
interface lag 100 multi-chassis
 no shutdown
 no routing
 lacp mode active
interface 1/1/1
 no shutdown
 no routing
interface 1/1/2
 no shutdown
 lag 100
interface 1/1/3
 no shutdown
 ip address 192.168.1.2/24
interface vlan100
 no shutdown
 ip address 192.168.1.1/24
 active-gateway ip 192.168.1.253 mac 00:00:00:00:00:01
 active-gateway ipv6 fe80::01 mac 00:00:00:01:00:01
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show running-config vsx

show running-config vsx

## Description

Displays the configured VSX commands.

## Example

```
switch# show running-config vsx
vsx
 system-mac 10:00:00:00:00:01
 inter-switch-link hello-interval 2
 inter-switch-link dead-interval 3
 inter-switch-link hold-time 3
 inter-switch-link peer-detect-interval 300
 role primary
```

```

 keepalive udp-port 1500
 keepalive hello-interval 2
 keepalive dead-interval 4
 keepalive peer 192.168.1.1 source 192.168.1.2
 inter-switch-link 1/1/43
interface lag 100 multi-chassis
 no shutdown
 no routing
 vlan access 1
 lacp mode active
interface 1/1/44
 no shutdown
 lag 100
interface vlan2
 ip address 10.0.0.2/24
 vsx-sync active-gateways
 active-gateway ip mac 00:aa:bb:dd:ee:ff
 active-gateway ip 10.0.0.1
 ipv6 address 2000:0:0:1::1/64
 ipv6 address 3000:0:0:1::1/64
 active-gateway ipv6 mac 00:aa:aa:aa:aa:ab
 active-gateway ipv6 2000:0:0:1::3
 active-gateway ipv6 3000:0:0:1::3
interface vlan3
 ipv6 address link-local fe80::100/64
 active-gateway ip mac 00:aa:bb:dd:ee:ff
 active-gateway ip 10.0.0.1
 active-gateway ipv6 mac 00:aa:aa:aa:aa:ab
 active-gateway ipv6 fe80::100
interface vlan4
 active-gateway ip mac 00:aa:bb:dd:ee:ff
 active-gateway ip 10.0.0.1
interface vlan5
 vsx active-forwarding

```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification                                                                                                      |
|------------------|-------------------------------------------------------------------------------------------------------------------|
| 10.09.0010       | Command will now display results for configurations where the active gateway and SVI share the same IPv6 address. |
| 10.07 or earlier | --                                                                                                                |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show running-config vsx-sync

show running-config vsx-sync



## Description

Displays the lines of running-configuration that VSX configuration synchronization is enabled on. The command also provides a rolled-up view of configuration expected to be synced. This command can be run from the primary or secondary peer.

## Example

Displaying the running configuration on which VSX synchronization is enabled:

```
switch# show running-config vsx-sync
Current vsx-sync configuration:
vlan 3
 vsx-sync
access-list ip test1
 vsx-sync
!
policy test2
 vsx-sync
!
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show running-config vsx-sync peer-diff

show running-config vsx-sync peer-diff

## Description

Displays the difference between the configuration of features enabled for VSX synchronization on the primary and secondary switches.

## Usage

Use this command for diagnosing errors. This command provides visibility into which configuration lines did not synchronize from the primary peer to the secondary peer. This command can be run from the primary or secondary peer. The output is displayed in the GNU diff unified format.

## Example

Displaying the running configuration on which VSX synchronization is enabled:

```
switch# show running-config vsx-sync peer-diff
--- /tmp/running-config-vsx.83e 2018-05-01 17:03:38.083281976 +0000
+++ /tmp/peer-running-config-vsx.83e 2018-05-01 17:03:38.077281976 +0000
@@ -1,4 +0,0 @@
-access-list ip sync
- vsx-sync
- !
- 10 permit any any any
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx active-forwarding

show vsx active-forwarding [interface <INTERFACE-VLAN>] [vsx-peer]

### Description

Shows all the VSX active-forwarding configured interface VLANs or the VSX active-forwarding peer information for a particular interface VLAN.

| Parameter                  | Description                                                                                                                                                                                                                      |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface <INTERFACE-VLAN> | Specifies the interface VLAN name. Syntax: string                                                                                                                                                                                |
| vsx-peer                   | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Displaying a list of VSX active-forwarding enabled interfaces:

```
switch# show vsx active-forwarding
List of VSX active-forwarding enabled interfaces:
vlan30
vlan32
vlan33
```

Displaying the VSX active-forwarding peer information for `vlan30`:

```
switch# show vsx active-forwarding interface vlan30
Interface vlan30 has VSX active-forwarding enabled.
Interface vlan30 Peer Data:
Peer MAC: 94:f1:28:21:22:00
Peer IPv6 Addresses:
 fe80::96f1:28ff:fe21:2200
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx brief

`show vsx brief [vsx-peer]`

### Description

Displays the brief VSX status.

| Parameter             | Description                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>vsx-peer</code> | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Usage

The `show vsx brief` command displays the ISLP device protocol states under the "Device State" heading.

**Table 1:** ISLP device protocol states

| Device state     | Definition                                                                                                                         |
|------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Peer-Established | The VSX switch is in a steady state. VSX LAGs are up.                                                                              |
| Sync-Primary     | ISL connectivity to the peer VSX switch is restored, and the VSX switch is syncing states to the peer VSX switch. VSX LAGs are up. |

| Device state                | Definition                                                                                                                                         |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Sync-Secondary              | ISL connectivity to the peer VSX switch is restored, and the VSX switch is learning states from the peer VSX switch. VSX LAGs are down.            |
| Sync-Secondary-Linkup-Delay | The VSX switch has learned its states from the peer VSX switch, and the VSX switch is monitoring for hardware to be programmed. VSX LAGs are down. |
| Split-System-Primary        | The VSX switch has lost ISL connectivity to the peer VSX switch. The VSX switch is operating as the primary VSX switch. VSX LAGs are up.           |
| Split-System-Secondary      | The VSX switch has lost ISL connectivity to the peer VSX switch. The VSX switch is operating as the secondary VSX switch. VSX LAGs are down.       |
| Waiting-For-Peer            | The VSX switch is waiting for connectivity to the peer VSX switch.                                                                                 |

## Example

Displaying the brief VSX status for the switch you are logged into:

```
vsx-primary# show vsx brief
ISL State : In-Sync
Device State : Peer-Established
Keepalive State : Keepalive-Established
Device Role : primary
Number of Multi-chassis LAG interfaces : 2
```

Displaying the brief VSX status for the peer (secondary) switch while entering the command on the primary switch:

```
vsx-primary# show vsx brief vsx-peer
ISL State : In-Sync
Device State : Peer-Established
Keepalive State : Keepalive-Established
Device Role : secondary
Number of Multi-chassis LAG interfaces : 2
```

Displaying the brief VSX status for the peer (primary) switch while entering the command on the secondary switch:

```
vsx-secondary# show vsx brief vsx-peer
ISL State : In-Sync
Device State : Peer-Established
Keepalive State : Keepalive-Established
Device Role : primary
Number of Multi-chassis LAG interfaces : 2
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx config-consistency

show vsx config-consistency [vsx-peer]

### Description

Displays the VSX global configuration consistency between two VSX switches.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Example

The following example shows a comparison between the two VSX switches.

```

switch# show vsx config-consistency
Configurations Local Peer

software version 0.1.0 0.1.0
ISL hello interval 1 1
ISL dead interval 5 5
ISL hold interval 0 0
ISL peer detect interval 300 300
Keepalive hello interval 1 1
Keepalive dead interval 3 3
Keepalive UDP port 7678 7678
System MAC 10:00:00:00:00:01
10:00:00:00:00:01

VSX VLAN List

Local ISL VLANs : 1,100
Peer ISL VLANs : 1,10

VSX Active Forwarding

Interface VLANs : 2, 5-9
Peer Interface VLANs : 2, 5-10

STP Configurations Local Peer

```

```

STP Enabled True True
STP Mode rpvst-auto rpvst-
auto
MST Config Name 10:00:00:00:00:01
10:00:00:00:00:01
MST Config Revision 0 0
MST Config Digest - -
MST hello time(in seconds) 2 2
MST maximum age(in seconds) 20 20
MST maximum hops 20 20
MST number of instances - -

RPVST VLAN List:

Local: 2,5-9
Peer : 2,5-9

...

```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vsx config-consistency lacp

`show vsx config-consistency lacp [<LAG-NAME>] [vsx-peer]`

## Description

Displays VSX LACP configuration consistency between two VSX switches.

| Parameter  | Description                                                                                                                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <LAG-NAME> | Specifies the LAG name. Optional. Syntax: string                                                                                                                                                                                 |
| vsx-peer   | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

```

switch# show vsx config-consistency lacp
Configurations

Name
Loop protect enabled
Hash scheme
Qos cos override
Qos dscp override
Qos trust

VSX VLAN list
1
Peer VSX VLAN list
1,10

STP link-type
STP port-type
STP bpdu-filter
STP bpdu-guard
STP loop-guard
STP root-guard
STP tcn-guard

Configurations

Name
Loop protect enabled
Hash scheme
Qos cos override
Qos dscp override
Qos trust
VSX VLAN list
1
Peer VSX VLAN list
1

STP link-type
STP port-type
STP bpdu-filter
STP bpdu-guard
STP loop-guard
STP root-guard
STP tcn-guard

```

| Configurations       | Local           | Peer            |
|----------------------|-----------------|-----------------|
| Name                 | lag100          | lag100          |
| Loop protect enabled | false           | true            |
| Hash scheme          | l2-src-dst-hash | l2-src-dst-hash |
| Qos cos override     | 0               | 0               |
| Qos dscp override    | 0               | 0               |
| Qos trust            |                 |                 |
| VSX VLAN list        |                 |                 |
| 1                    |                 |                 |
| Peer VSX VLAN list   |                 |                 |
| 1,10                 |                 |                 |
| STP link-type        | point-to-point  | point-to-point  |
| STP port-type        | admin-network   | admin-network   |
| STP bpdu-filter      | Disabled        | Disabled        |
| STP bpdu-guard       | Disabled        | Disabled        |
| STP loop-guard       | Disabled        | Disabled        |
| STP root-guard       | Disabled        | Disabled        |
| STP tcn-guard        | Disabled        | Disabled        |

| Configurations       | Local           | Peer            |
|----------------------|-----------------|-----------------|
| Name                 | lag111          | lag111          |
| Loop protect enabled | false           | false           |
| Hash scheme          | l2-src-dst-hash | l2-src-dst-hash |
| Qos cos override     | 0               | 0               |
| Qos dscp override    | 0               | 0               |
| Qos trust            |                 |                 |
| VSX VLAN list        |                 |                 |
| 1                    |                 |                 |
| Peer VSX VLAN list   |                 |                 |
| 1                    |                 |                 |
| STP link-type        | point-to-point  | point-to-point  |
| STP port-type        | admin-network   | admin-network   |
| STP bpdu-filter      | Disabled        | Disabled        |
| STP bpdu-guard       | Disabled        | Disabled        |
| STP loop-guard       | Disabled        | Disabled        |
| STP root-guard       | Disabled        | Disabled        |
| STP tcn-guard        | Disabled        | Disabled        |

```

switch (config-if-vlan)# show traffic-insight test monitor-type dns-average-
latency mon2

```

|                                 |               | error-statistics |          |             |
|---------------------------------|---------------|------------------|----------|-------------|
| Name                            |               | number_of_       | dns_name | dns_server_ |
| Type                            |               |                  |          |             |
| Start time for error monitoring |               |                  |          |             |
| End time for error monitoring   |               |                  |          |             |
| client_mac                      | dns_server_ip | number_of_       | dns_name | dns_server_ |
| format_                         |               |                  |          |             |
|                                 |               | dns_failures     | _errors  | failures    |
| errors                          |               |                  |          |             |
| -----                           |               |                  |          |             |
| -----                           |               |                  |          |             |
| aa:aa:aa:aa:aa:aa               | 172.0.0.1     | 200              | 50       | 100         |
| 50                              |               |                  |          |             |

|                         |           |     |    |    |
|-------------------------|-----------|-----|----|----|
| bb:bb:bb:bb:bb:bb<br>20 | 172.1.1.1 | 50  | 10 | 20 |
| cc:cc:cc:cc:cc:cc<br>50 | 172.2.2.2 | 150 | 75 | 25 |



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx configuration

```
show vsx configuration {inter-switch-link | keepalive} [vsx-peer]
```

### Description

Displays the ISL configuration or keepalive protocol configuration in VSX.

| Parameter                       | Description                                                                                                                                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| {inter-switch-link   keepalive} | Selects inter-switch-link or keepalive.                                                                                                                                                                                          |
| inter-switch-link               | Displays the ISL configuration in VSX.                                                                                                                                                                                           |
| keepalive                       | Displays the keepalive protocol configuration in VSX.                                                                                                                                                                            |
| vsx-peer                        | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Displaying the ISL configuration in VSX:

```
switch# show vsx configuration inter-switch-link
Inter Switch Link : 1/1/43
Hello Interval : 1 Seconds
Dead Interval : 20 Seconds
Hold Time : 0 Seconds
Peer detect interval : 300 Seconds
```



```
System MAC : 10:00:00:00:00:01
Device Role : primary
Multichassis LAGs : lag100
```

Displaying the keepalive protocol configuration in VSX:

```
switch# show vsx configuration keepalive
Keepalive Interface : 1/1/1
Keepalive VRF : test1
Source IP Address : 192.168.1.1
Peer IP Address : 192.168.1.2
UDP Port : 7678
Hello Interval : 1 Seconds
Dead Interval : 3 Seconds
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vsx configuration split-recovery

show vsx configuration split-recovery [vsx-peer]

## Description

Displays the state of the split recovery mode.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

```
switch# show vsx configuration split-recovery
Split Recovery Mode : Enabled
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vsx ip data-path

```
show vsx ip data-path [<IP-ADDR> | <IP-ADDR>/<MASK>] [vrf <VRF-NAME>] [vsx-peer]
```

## Description

Displays the datapath of the IPv4 route present on local and VSX peer devices.

| Parameter                     | Description                                                                                                                                                                                                                      |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP-ADDR>   <IP-ADDR>/<MASK>] | Selects one of the following: <IP-ADDR> or <IP-ADDR>/<MASK>                                                                                                                                                                      |
| <IP-ADDR>                     | Specifies the datapath for an IPv4 address based on the parameters provided.                                                                                                                                                     |
| <IP-ADDR>/<MASK>              | Specifies the datapath for an IPv4 address and its specified subnet. Optional. Syntax: A.B.C.D/M                                                                                                                                 |
| vrf <VRF-NAME>                | Shows the IPv4 datapath for a specified VRF.                                                                                                                                                                                     |
| vsx-peer                      | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

Displaying the datapath on a VSX switch for 192.0.2.0:

```
switch# show vsx ip data-path 192.0.2.0

IPv4 Data Path Information For 192.0.2.0

Local Device

Route : 192.0.2.0/32
 Egress L3 Interface : 1/1/2
```

```

Next Hop MAC Address : 08:00:09:ea:d7:d1
Egress Port : 1/1/2

Egress L3 Interface : 1/1/3
Nexthop Hop MAC Address : 08:00:09:8e:59:1d
Egress Port : 1/1/3

Peer Device

Route : 192.0.2.0/32
Egress L3 Interface : loopback1

```

Displaying the datapath on a VSX switch for 198.51.100.0/32:

```

switch# show vsx ip data-path 198.51.100.0/32

IPv4 Data Path Information For 198.51.100.0/32

Local Device

Route : 198.51.100.0/32
Egress L3 Interface : 1/1/4

```

Displaying the datapaths on a VSX switch for 198.51.100.1:

```

switch# show vsx ip data-path 198.51.100.1

IPv4 Data Path Information For 198.51.100.1

Local Device

Route : 198.51.100.1/32
Egress L3 Interface : 1/1/4

Peer Device

Route : 198.51.100.0/24
Egress L3 Interface : 1/1/2
Next Hop MAC Address : 08:00:09:db:21:e8
Egress Port : 1/1/2

```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

# show vsx ip route

show vsx ip route [<IP-ADDR> | <IP-ADDR>/<MASK> | unique] [vrf <VRF-NAME> | all-vrfs] [vsx-peer]

## Description

Displays a specified LAG or all configured LAGs along with VSX LAGs.

| Parameter                              | Description                                                                                                                                                                                                                      |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IP-ADDR>   <IP-ADDR>/<MASK>   unique] | Selects one of the following: <IP-ADDR>, <IP-ADDR>/<MASK>, or unique                                                                                                                                                             |
| <IP-ADDR>                              | Specifies the route information for an IPv4 address based on the parameters provided.                                                                                                                                            |
| <IP-ADDR>/<MASK>                       | Specifies the route information for an IPv4 address and its specified subnet. Optional. Syntax: A.B.C.D/M                                                                                                                        |
| unique                                 | Specifies routes that are present only on the primary switch or only on the secondary switch. The routes that are present on both the primary and secondary switch are excluded. Optional. Syntax string.                        |
| vrf <VRF-NAME>   all-vrfs              | Selects the VRF name or all VRFs.                                                                                                                                                                                                |
| <VRF-NAME>                             | Shows the IPv4 route information for a specified VRF.                                                                                                                                                                            |
| all-vrf                                | Shows the IPv4 route information for all VRFs.                                                                                                                                                                                   |
| vsx-peer                               | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Displaying IPv4 routes on a VSX switch:

```
switch# show vsx ip route

IPv4 Forwarding Routes

'[x/y]' denotes [distance/metric]

192.0.2.0/32, vrf default
 via 192.0.2.1, [1/0], static on vsx1
 via 192.0.2.2, [1/0], static on vsx2
```

Displaying IPv4 routes on a VSX switch:

```
switch# show vsx ip route

IPv4 Forwarding Routes

'[x/y]' denotes [distance/metric]
```

```

192.0.2.3/24, vrf default
 via 1/1/3, [0/0], connected on vsx1
 via 192.0.2.2, [110/2], ospf on vsx2
192.0.2.4/32, vrf default
 via 1/1/3, [0/0], local on vsx1
192.0.2.5/24, vrf default
 via 1/1/4, [0/0], connected on vsx1
 via 192.0.2.2, [110/3], ospf on vsx2
192.0.2.6/32, vrf default
 via 1/1/4, [0/0], local on vsx1
192.0.2.7/32, vrf default
 via 192.0.2.8, [110/1], ospf on vsx1
 via 192.0.2.1, [110/1], ospf on vsx1
 via loopback1, [0/0], local on vsx2

```

Displaying IPv4 unique routes on a VSX switch:

```

switch# show vsx ip route unique

IPv4 Forwarding Routes

'[x/y]' denotes [distance/metric]

192.0.2.0/32, vrf default
 via 192.0.2.2, [1/0], static on vsx2
192.0.2.9/32, vrf default
 via 192.0.2.1, [1/0], static on vsx1

```

Displaying IPv4 routes on a VSX switch for 192.0.2.10:

```

switch# show vsx ip route 192.0.2.10

IPv4 Forwarding Routes

'[x/y]' denotes [distance/metric]

192.0.2.10/32, vrf default
 via 192.0.2.1, [1/0], static on vsx1
 via 192.0.2.2, [1/0], static on vsx2

```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx ipv6 data-path

show vsx ipv6 data-path [<IPv6-ADDR> | <IPv6-ADDR>/<MASK>] [vrf <VRF-NAME>] [vsx-peer]

### Description

Displays the datapath of the IPv6 route on local and peer VSX devices.

| Parameter                         | Description                                                                                                                                                                                                                      |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv6-ADDR>   <IPv6-ADDR>/<MASK>] | Selects one of the following: <IPv6-ADDR> or <IPv6-ADDR>/<MASK>                                                                                                                                                                  |
| <IPv6-ADDR>                       | Specifies the datapath for an IPv6 address based on the parameters provided.                                                                                                                                                     |
| <IPv6-ADDR>/<MASK>                | Specifies the datapath for an IPv6 address and its specified subnet. Optional. Syntax: A.B.C.D/M                                                                                                                                 |
| vrf <VRF-NAME>                    | Shows the IPv6 datapath for a specified VRF.                                                                                                                                                                                     |
| vsx-peer                          | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

### Examples

Displaying an IPv6 datapath on a VSX switch:

```
switch# show vsx ipv6 data-path 1000::

IPv6 Data Path Information For 1000::

Local Device

Route : 1000::/64
 Egress L3 Interface : 1/1/2

Peer Device

Route : 1000::/64
 Egress L3 Interface : 1/1/2
```

Displaying an IPv6 datapath on a VSX switch:

```
switch# show vsx ipv6 data-path 2000::

IPv6 Data Path Information For 2000::

Local Device
```

```

Route : 2000::/64
 Egress L3 Interface : 1/1/2
 Next Hop MAC Address : 08:00:09:0e:0c:1b
 Egress Port : 1/1/2
```

Displaying IPv6 datapath for 3000::/64 on a VSX switch:

```
switch# show vsx ipv6 data-path 3000::/64
IPv6 Data Path Information For 3000::/64

Local Device

Route : 3000::/64
 Egress L3 Interface : 1/1/2
 Next Hop MAC Address : 08:00:09:0e:0c:1b
 Egress Port : 1/1/2
IPv6 Data Path Information For 3000::/64

Local Device

Route : 3000::/64
 Egress L3 Interface : 1/1/2
 Next Hop MAC Address : 08:00:09:0e:0c:1b
 Egress Port : 1/1/2
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx ipv6 route

```
show vsx ipv6 route [<IPv6-ADDR> | <IPv6-ADDR>/<MASK> | unique]
[vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

## Description

Displays a specified LAG or all configured LAGs along with VSX LAGs.

| Parameter                                                                | Description                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;IPV6-ADDR&gt;   &lt;IPV6-ADDR&gt;/&lt;MASK&gt;   unique</code> | Selects one of the following: <code>&lt;IPV6-ADDR&gt;</code> , <code>&lt;IPV6-ADDR&gt;/&lt;MASK&gt;</code> , or <code>unique</code>                                                                                              |
| <code>&lt;IPV6-ADDR&gt;</code>                                           | Specifies the route information for an IPv4 address based on the parameters provided.                                                                                                                                            |
| <code>&lt;IPV6-ADDR&gt;/&lt;MASK&gt;</code>                              | Specifies the route information for an IPv4 address and its specified subnet. Optional. Syntax: A.B.C.D/M                                                                                                                        |
| <code>unique</code>                                                      | Specifies routes that are present only on the primary switch or only on the secondary switch. The routes that are present on both the primary and secondary switch are excluded. Optional. Syntax string.                        |
| <code>vrf &lt;VRF-NAME&gt;   all-vrfs</code>                             | Selects the VRF name or all VRFs.                                                                                                                                                                                                |
| <code>&lt;VRF-NAME&gt;</code>                                            | Shows the IPv4 route information for a specified VRF.                                                                                                                                                                            |
| <code>all-vrf</code>                                                     | Shows the IPv4 route information for all VRFs.                                                                                                                                                                                   |
| <code>vsx-peer</code>                                                    | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Examples

Displaying IPv6 routes on a VSX switch:

```
switch# show vsx ipv6 route

IPv6 Forwarding Routes

'[x/y]' denotes [distance/metric]

1000::/64, vrf default
 via 1/1/2, [0/0], connected on vsx1
 via 1/1/2, [0/0], connected on vsx2
1000::1/128, vrf default
 via 1/1/2, [0/0], local on vsx1
```

Displaying IPv6 unique routes on a VSX switch:

```
switch# show vsx ipv6 route unique

IPv6 Forwarding Routes

'[x/y]' denotes [distance/metric]

1000::1/128, vrf default
 via 1/1/2, [0/0], local on vsx1
1000::2/128, vrf default
 via 1/1/2, [0/0], local on vsx2
3000::/64, vrf default
```



```
via 1000::2, [1/0], static on vsx1
```

Displaying IPv6 routes on a VSX switch for 2000::/64:

```
switch# show vsx ipv6 route 2000::/64
IPv6 Forwarding Routes

'[x/y]' denotes [distance/metric]

2000::/64, vrf default
 via 1000::2, [1/0], static on vsx1
 via 1000::1, [1/0], static on vsx2
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx status

```
show vsx status [inter-switch-link | keepalive | linkup-delay] [vsx-peer]
```

### Description

Displays global VSX status or a specified status determined by the selected parameter.

| Parameter                                      | Description                                                                                                                                                                          |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [inter-switch-link   keepalive   linkup-delay] | Selects one of the following: inter-switch-link, keepalive, or linkup-delay                                                                                                          |
| inter-switch-link                              | Specifies the display of the ISL status in VSX.                                                                                                                                      |
| keepalive                                      | Specifies the display of the VSX keepalive protocol status.                                                                                                                          |
| linkup-delay                                   | Specifies the display of the VSX link-up delay information, such as the: <ul style="list-style-type: none"><li>Configured link-up delay timer.</li><li>Delay timer status.</li></ul> |

| Parameter | Description                                                                                                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <ul style="list-style-type: none"> <li>Initial sync status.</li> <li>LAGs on which the delay timer is running.</li> <li>Status of the LAGs excluded from the link-up delay timer.</li> <li>Interfaces that are shut down during VSX split.</li> <li>Interfaces that are shut down during VSX split</li> </ul> |
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.                                                                              |

## Examples

Displaying the global VSX status:

```
switch# show vsx status
VSX Operational State

ISL channel : In-Sync
ISL mgmt channel : operational
Config Sync Status : in-sync
NAE : peer_reachable
HTTPS Server : peer_reachable

Attribute Local Peer

ISL link 1/1/43 1/1/43
ISL version 2 2
System MAC 48:0f:cf:af:70:84 48:0f:cf:af:c2:84
Platform 8320 8320
Software Version 10.0x.xxxx 10.0x.xxxx
Device Role primary secondary
```

Displaying the ISL status in VSX:

```
switch# show vsx status inter-switch-link
State : In-Sync
Link Status : up
Mgmt state : operational

Inter-switch link Statistics

Hello Packets Tx : 4572
Hello Packets Rx : 4573
Data Packets Tx : 80634
Data Packets Rx : 80637
Mgmt Packets Tx : 25946
Mgmt Packets Rx : 25167
Mgmt Packet Drops : 0
```

Displaying the VSX keepalive protocol status:

```

switch# show vsx status keepalive
Keepalive State : Keepalive-Established
Last Established : Thu Jun 8 09:03:01 2018
Last Failed : Thu Jun 8 09:04:02 2018
Peer System Id : 58:1f:cf:af:a0:84
Peer Device Role : primary

Keepalive Counters
Keepalive Packets Tx : 322
Keepalive Packets Rx : 121
Keepalive Timeouts : 0
Keepalive Packets Dropped : 14

```

Displaying the VSX link-up delay status while ARP/MAC VSX synchronization is in progress:

```

switch# show vsx status linkup-delay

Configured linkup delay-timer : 180 seconds
Initial sync status : In-progress
Delay timer status : Waiting-to-start
Linkup Delay time left :
Interfaces that will be brought up after delay timer expires : lag20,lag30-lag31
Interfaces enabled for shutdown-on-split that will be brought
up after the delay timer expires :
Interfaces that are excluded from delay timer : lag2

```

Displaying the VSX link-up delay status with ARP/MAC VSX synchronization completed with the delay timer running:

```

switch# show vsx status linkup-delay

Configured linkup delay-timer : 180 seconds
Initial sync status : Completed
Delay timer status : Running
Linkup Delay time left : 1 minutes 22
seconds
Interfaces that will be brought up after delay timer expires : lag20,lag30-lag31
Interfaces enabled for shutdown-on-split that will be brought
up after the delay timer expires :
Interfaces that are excluded from delay timer : lag2

```

Displaying the VSX link-up delay status with ARP/MAC VSX synchronization completed and the delay timer expired:

Displaying the global VSX status for the peer switch:

```

vsx-primary# show vsx status vsx-peer
VSX Operational State

ISL channel : In-Sync
ISL mgmt channel : operational
Config Sync Status : in-sync
NAE : peer_reachable

```

```

HTTPS Server : peer_reachable

Attribute Local Peer

ISL link lag1 lag1
ISL version 2 2
System MAC e0:07:1b:cb:72:e4 98:f2:b3:68:79:2e
Platform 8320 8320
Software Version 10.0x.xxxx 10.0x.xxxx
Device Role secondary primary

```

Displaying the status for an out-of-sync status for VSX.

```

switch# show vsx status linkup-delay

Configured linkup delay-timer : 20 seconds
Initial sync status :
Delay timer status :
Linkup Delay time left :
Interfaces that will be brought up after delay timer expires :
Interfaces enabled for shutdown-on-split that will be brought
up after the delay timer expires :
Interfaces that are excluded from delay timer :

```

Displaying the status VSX link-up delay status when interfaces enabled for shutdown-on-split.

```

switch# show vsx status linkup-delay

Configured linkup delay-timer : 180 seconds
Initial sync status : In-progress
Delay timer status : Waiting-to-start
Linkup Delay time left :
Interfaces that will be brought up after delay timer expires : lag8,lag256
Interfaces enabled for shutdown-on-split that will be brought
up after the delay timer expires : 1/1/27,1/1/37,
 vlan2-vlan57
Interfaces that are excluded from delay timer :

```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                | Authority                                                                                                                                                              |
|---------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager<br>(#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vsx status config-sync

show vsx status config-sync [vsx-peer]

## Description

Displays VSX configuration synchronization status for peers. This command can be run from the primary or secondary peer to view the configuration synchronization state.

| Parameter | Description                                                                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vsx-peer  | Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX. |

## Example

```
switch# show vsx status config-sync
Admin State : Enabled
Operational State : Operational
Error State : None
Recommended remediation : N/A
Current Time : Wed Jul 18 23:41:07 2018
Last Sync Time : Wed Jul 18 23:38:26 2018
```



The Admin State parameter can be configured individually on each of the switches on the VSX pair. Hence difference in values does not imply a failure.



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show vsx status peering

show vsx status peering

## Description

Displays synchronization peering status and hardware peering status for modules such as MAC, neighbor, spanning-tree, and route. This command can be used to view the status of VSX peering, following a VSX device reboot or an ISL flap.

Following are the possible values for VSX peering status:

- **Complete**—VSX peering process is successfully completed.
- **In-progress**—VSX peering is being processed.
- **Not-started**—VSX peering process is yet to be started.

## Examples

Displaying the VSX peering status :

```
switch# show vsx status peering

Module Sync-Status Hardware-Status

MAC In-progress Not-started
Neighbor Complete In-progress
Route Complete Complete
Spanning-tree In-progress Not-started
EVPN In-progress Not-started
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show vsx status shutdown-on-split

```
show vsx status shutdown-on-split
```

### Description

Displays the status of the interfaces that are shut down during a VSX split.



You can also use `show interface` command to view the status of the interface. For example, assume that you have shut down the non-vsx interface 1/1/2 during the VSX split. When you enter `show interface` command on the secondary switch, the output from the command indicates that the interface was blocked by VSX feature.

## Examples

Displaying the status of interfaces that are shut down during the VSX split:

```
switch(config)# show vsx status shutdown-on-split
List of non-vsx interfaces enabled for split shutdown and its status.
```

| Interfaces | Status   |
|------------|----------|
| 1/1/1      | Disabled |
| lag100     | Disabled |
| vlan2      | Disabled |



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## split recovery

split-recovery  
no split-recovery

### Description

Enables split recovery mode. Split recovery mode is enabled by default.

The **no** form of this command disables split-recovery mode.

### Usage

Split recovery mode prevents traffic loss when the ISL goes out-of-sync and keepalive subsequently fails. When the ISL goes out-of-sync and keepalive is established, the secondary VSX LAGs are brought down. If keepalive then also fails, this situation causes a split condition. In this case, if split recovery mode is enabled, the secondary switch restores its VSX LAGs so they are up.

When split recovery mode is disabled during a split condition, the secondary switch keeps its VSX LAGs down.

### Examples

Enabling split recovery mode:

```
switch(config-vsx)# split-recovery
```

Disabling split recovery mode:

```
switch(config-vsx)# no split-recovery
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## system-mac

```
system-mac <MAC-ADDR>
no system-mac [<MAC-ADDR>]
```

### Description

Sets the MAC address as the VSX system MAC address to be used by control plane protocols, such as STP and LACP. A pair of VSX switches must have the same VSX system MAC.

The **no** form of this command unconfigures the VSX system MAC address to be used by control plane protocols.

| Parameter  | Description                                                                                                    |
|------------|----------------------------------------------------------------------------------------------------------------|
| <MAC-ADDR> | Specifies the MAC address in a colon separated format, such as XX:XX:XX:XX:XX:XX, for control plane protocols. |

### Usage

The **system-mac <MAC-ADDR>** command is highly recommended for preventing traffic disruptions when the primary VSX switch restores after the secondary VSX switch, such as during:

- A primary switch hardware replacement.
- A power outage with the primary switch restore after the secondary switch restore.

When the primary switch is restored after the secondary switch, a traffic disruption might occur when the ISL starts to sync. This situation occurs because the MAC system address changes from the secondary switch to the primary switch for the LACP. To avoid the traffic disruption, set the common system MAC address by entering the **system-mac <MAC-ADDR>** command. This command creates a common system MAC address between the two VSX switches. This common system MAC address prevents a traffic disruption when the secondary switch comes up before the primary switch. If the common system MAC access is enabled, the secondary switch uses the common system MAC address instead of its own system MAC address, which prevents a traffic loss.



The system MAC address also maintains the same MSTP bridge ID across VSX switches, which act as a single switch.

## Examples

Setting a MAC address as the VSX system MAC address to be used by control plane protocols:

```
switch(config-vsx) # system-mac 02:01:00:00:01:00
```

Unconfiguring a VSX system MAC address to be used by control plane protocols:

```
switch(config-vsx) # no system-mac 02:01:00:00:01:00
```



Null system MAC address such as 00:00:00:00:00:00 is not allowed.



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification                           |
|------------------|----------------------------------------|
| 10.08            | Updated <b>no</b> form of the command. |
| 10.07 or earlier | --                                     |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## VSX

```
vsx
no vsx
```

## Description

Creates the VSX context on the switch.

The **no** form of this command disables the VSX context on the switch and removes all related configuration settings.

## Examples

Creating the VSX context on the switch:

```
switch(config) # vsx
switch(config-vsx) #
```

Removing the VSX context and all VSX configuration settings from the switch:

```
switch(config-vsx)# no vsx
VSX configuration will be deleted.
Do you want to continue (y/n)? y
switch(config)#
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## vsx active-forwarding

```
vsx active-forwarding
no vsx active-forwarding
```

### Description

Configures VSX active-forwarding on an interface VLAN.

The **no** form of this command unconfigures VSX active-forwarding on a VLAN interface.

### Usage

Active forwarding cannot be configured when ICMP redirect is enabled. The ICMP redirect setting is global not per SVI. Enter the `no ip icmp redirect` command for disabling ICMP redirect at the `switch (config)#` prompt.

If a system has active forwarding enabled, an active gateway can have a maximum of 14 "unique" MAC addresses per system, including IPv4 and IPv6 addresses.

If a system has active forwarding disabled, an active gateway can have a maximum of 16 "unique" MAC addresses per system, including IPv4 and IPv6 addresses.

### Examples

Successfully enabling VSX active-forwarding:

```
switch# interface vlan 3
switch(config-if-vlan)# vsx active-forwarding
switch(config-vsx)#
```

Unconfiguring VSX active-forwarding:

```
switch# interface vlan 3
switch(config-if-vlan)# no vsx active-forwarding
switch(config-vsx)#
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Administrators or local user group members with execution rights for this command. |

## vsx shutdown-on-split

```
vsx shutdown-on-split
no vsx shutdown-on-split
```

### Description

Shuts down the configured non-VSX interfaces on the VSX secondary along with VSX interfaces during a VSX split.

The **no** form of this command resumes the non-VSX interfaces that are shut down during the VSX split.



This command has no effect on the VSX primary during a split. However, when applied on the VSX primary, the command will bring down the non-VSX interfaces until linkup delay timer expires during the VSX primary reboot.

## Examples

Shutting down the non-VSX interface 1/1/1 during the VSX split:

```
switch(config)# interface 1/1/1
switch(config-if)# vsx shutdown-on-split
switch(config)# interface lag 1
switch(config-lag-if)# vsx shutdown-on-split
```

Shutting down the non-VSX interface LAG 5 during the VSX split:

```
switch(config)# interface lag 5
switch(config-lag-if)# vsx shutdown-on-split
```

Shutting down the non-VSX SVI during the VSX split:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# vsx shutdown-on-split
```

Resuming the non-VSX interface that are shutdown during the VSX split:

```
switch(config-if)# no vsx shutdown-on-split
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                              | Authority                                                                          |
|---------------|----------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if<br>config-lag-if<br>config-if-vlan | Administrators or local user group members with execution rights for this command. |

## vsx-sync

```
vsx-sync
no vsx-sync
```

### Description

Enables VSX synchronization for the entire context for the following features from the primary VSX node to the secondary peer switch:

- Access list context
- Classifier context
- Object group context
- Policy-based routing profile context
- Policy context
- QoS queue profile context
- QoS schedule profile context
- VLAN context

The **no** form of this command disables VSX synchronization for the entire context for a feature, but it does not remove the feature configurations from the secondary peer. Any subsequent configuration changes made under the specific configuration context are not synchronized to the secondary peer switch.

### Usage

Make sure that you are in the correct context for the feature that you are trying to enable VSX synchronization:

| Feature context for enabling VSX synchronization                 | Command for accessing correct context for the <i>vsx-sync</i> command* |
|------------------------------------------------------------------|------------------------------------------------------------------------|
| Access list context for an ACL type, such as IPv4, IPv6, or MAC. | <code>access-list &lt;ACL-TYPE&gt; &lt;ACL-NAME&gt;</code>             |
| Class context for a class type, such as IPv4, IPv6, or MAC.      | <code>class &lt;CLASS-TYPE&gt; &lt;CLASS-NAME&gt;</code>               |
| Object group context for IPv4                                    | <code>object-group ip address &lt;OBJECT-GROUP-NAME&gt;</code>         |
| Object group context for IPv6                                    | <code>object-group ipv6 address &lt;OBJECT-GROUP-NAME&gt;</code>       |
| Object group context for ports                                   | <code>object-group port &lt;OBJECT-GROUP-NAME&gt;</code>               |
| Policy-based routing profile context                             | <code>pbr &lt;ACTION-LIST-NAME&gt;</code>                              |
| Policy context                                                   | <code>policy &lt;POLICY-NAME&gt;</code>                                |
| QoS queue profile context                                        | <code>qos queue-profile &lt;QUEUE-PROFILE-NAME&gt;</code>              |
| QoS schedule profile context                                     | <code>qos schedule-profile &lt;SCHEDULE-PROFILE-NAME&gt;</code>        |
| VLAN context                                                     | <code>vlan &lt;ID&gt;</code>                                           |

\*The commands listed in this column are entered at the `switch(config)#` prompt, as shown in the following examples.

## Examples

Enabling VSX synchronization for this IPv4 access list context to the secondary peer:

```
switch(config)# access-list ip ITBoston
switch(config-acl-ip)# vsx-sync
```

Enabling VSX synchronization for this IPv6 access list context to the secondary peer:

```
switch(config)# access-list ipv6 ITRoseville
switch(config-acl-ipv6)# vsx-sync
```

Enabling VSX synchronization for this MAC access list context to the secondary peer:

```
switch(config)# access-list mac ITBangalore
switch(config-acl-ipv6)# vsx-sync
```

Enabling VSX synchronization for this IPv4 class context to the secondary peer:

```
switch(config)# class ip ITengineering
switch(config-class-ip)# vsx-sync
```

Enabling VSX synchronization for this object group context for IPv4:

```
switch(config)# object-group ip address group1
switch(config-addrgroup-ip)# 1.1.1.1
switch(config-addrgroup-ip)# vsx-sync
```

Enabling VSX synchronization for this QoS queue profile context to the secondary peer:

```
switch(config)# qos queue-profile test_queue_profile
switch(config-queue)# vsx-sync
```

Enabling VSX synchronization for this QoS schedule profile context to the secondary peer:

```
switch(config)# qos schedule-profile test_queue_profile1
switch(config-schedule)# vsx-sync
```

Enabling VSX synchronization for this PBR profile context to the secondary peer:

```
switch(config)# pbr engineering
switch(config-pbr-action-list-engineering)# vsx-sync
```

Enabling VSX synchronization for this policy context to the secondary peer:

```
switch(config)# policy ITPaloAlto
switch(config-policy)# vsx-sync
```

Enabling VSX synchronization for this VLAN context to the secondary peer:

```
switch(config)# vlan 1
switch(config-vlan-1)# vsx-sync
```

Disabling VSX synchronization for this IPv4 class context to the secondary peer:

```
switch(config)# class ip ITengineering
switch(config-class-ip)# no vsx-sync
```

Disabling VSX synchronization for this object group context for IPv4:

```
switch(config)# object-group ip address group1
switch(config-addrgroup-ip)# no vsx-sync
```

Disabling VSX synchronization for this QoS queue profile context to the secondary peer:

```
switch(config)# qos queue-profile test_queue_profile
switch(config-queue)# no vsx-sync
```

Disabling VSX synchronization for this QoS schedule profile context to the secondary peer:

```
switch(config)# qos schedule-profile test_queue_profile1
switch(config-schedule)# no vsx-sync
```

Disabling VSX synchronization for this PBR profile context to the secondary peer:

```
switch(config)# pbr engineering
switch(config-pbr-action-list-engineering)# no vsx-sync
```

Disabling VSX synchronization for this policy context to the secondary peer:

```
switch(config)# policy ITPaloAlto
switch(config-policy)# no vsx-sync
```

Disabling VSX synchronization for this MAC access list context to the secondary peer:

```
switch(config)# access-list mac ITBangalore
switch(config-acl-ipv6)# no vsx-sync
```

Disabling VSX synchronization for this VLAN context to the secondary peer:

```
switch(config)# vlan 1
switch(config-vlan-1)# no vsx-sync
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context                                                                                                                                                                                      | Authority                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-acl-<ACL-TYPE><br>config-addrgroup-ip<br>config-addrgroup-ipv6<br>config-class-<CLASS-TYPE><br>config-policy<br>config-portgroup<br>config-pbr-action-list-<ACTION-LIST-NAME><br>config-queue | Administrators or local user group members with execution rights for this command. |

```
config-schedule-<NAME>
config-vlan-<VLAN-ID>
```

## vsx-sync (config-if, config-lag-if contexts)

```
vsx-sync {[access-lists] [qos] [rate-limits] [vlans] [policies] [irdp] [portfilter]
[private-vlan port-type] [dhcp-snooping]]
no vsx-sync {[access-lists] [qos] [rate-limits] [vlans] [policies] [irdp] [portfilter]
[private-vlan port-type] [dhcp-snooping]]
```

### Description

Enables VSX synchronization for the following for a logical interface or a LAG instance:

- Access lists
- IRDP configurations
- QoS
- Rate limits
- Port filter configurations
- VLAN associations
- PVLAN port type configurations
- DHCP snooping

This command enables VSX synchronization for individual associations and to the combination of associations to the interface context. To synchronize the associations, you must configure the same interface on the peer switch.



When enabling VSX synchronization under a physical interface, under a VLAN interface, or a VSX LAG, create on the secondary switch the physical interface, VLAN interface, or VSX LAG with the same name and routing setting as on the primary switch. For example, if the primary switch has a physical interface of 1/1/1, you must create another physical interface of 1/1/1 on the secondary switch. Also, if the primary VSX switch has routing enabled, the secondary switch must have routing enabled. Once the name and routing information is the same, VSX synchronization synchronizes the additional configuration information from the primary VSX switch to the secondary VSX switch.

The **no** form of this command disables VSX synchronization, but it does not remove the feature configurations from the secondary peer.

| Parameter    | Description                                                                                 |
|--------------|---------------------------------------------------------------------------------------------|
| access-lists | Specifies the access lists that are associated under the interface enabled for VSX syncing. |
| qos          | Specifies the QoS associated under the interface enabled for VSX syncing.                   |
| rate-limits  | Specifies the rate limits that are associated under the interface enabled for VSX syncing.  |



| Parameter              | Description                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vlan                   | Specifies the VLANs that are associated under the interface enabled for VSX syncing.                                                                             |
| policy                 | Specifies the classifier policies that are associated under the interface enabled for VSX syncing.                                                               |
| irdp                   | Specifies the Internet Router Discovery Protocol (IRDP) configurations that are associated under the interface enabled for VSX syncing.                          |
| portfilter             | Specifies the port filter configurations that are associated under the interface enabled for VSX syncing.                                                        |
| private-vlan port-type | Specifies the PVLAN port type configurations that are associated under the interface enabled for VSX syncing.                                                    |
| dhcp-snooping          | Specifies the DHCP snooping configuration parameters that are associated under the interface enabled for VSX syncing.                                            |
| macsec                 | For switches that support MACsec, this parameter specifies the MACsec and MKA policy parameters that are associated under the interface enabled for VSX syncing. |

## Example

Enabling VSX synchronization for VLANs associated with logical interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# vsx-sync vlan
```

Enabling VSX synchronization for access lists associated with logical interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# vsx-sync access-lists
```

Enabling VSX synchronization for access lists and policies that are associated with logical interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# vsx-sync access-lists policy
```

Enabling VSX synchronization for VLANs and QoS that are associated under logical interface 1/1/5:

```
switch(config)# interface 1/1/5
switch(config-if)# vsx-sync vlans qos
```

Enabling VSX synchronization for rate limits that are associated under logical interface 1/1/5:

```
switch(config)# interface 1/1/5
switch(config-if)# vsx-sync rate-limits
```

Enabling VSX synchronization for rate limits, VLANs, QoS, access lists, policies associated with logical interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# vsx-sync rate-limits vlans qos access-lists policies
```

Enabling VSX synchronization for VLAN 1 under interface LAG 1:

```
switch(config)# interface lag 1
switch(config-lag-if)# vsx-sync vlans
switch(config-lag-if)# vlan trunk native 1
```

Enabling VSX synchronization for an access list under interface LAG 2:

```
switch(config)# interface lag 2
switch(config-lag-if)# vsx-sync access-lists
switch(config-lag-if)# apply access-list ip test1 in
```

Enabling VSX synchronization for a QoS under interface LAG 3:

```
switch(config)# interface lag 3
switch(config-lag-if)# vsx-sync qos
switch(config-lag-if)# apply qos schedule-profile test
```

Enabling VSX synchronization for a rate limit under interface LAG 4:

```
switch(config)# interface lag 4
switch(config-lag-if)# vsx-sync rate-limits
switch(config-lag-if)# rate-limit broadcast 23 kbps
```

Enabling VSX synchronization for a policy named test under interface LAG 5:

```
switch(config)# interface lag 5
switch(config-lag-if)# vsx-sync policies
switch(config-lag-if)# apply policy test in
```

Enabling VSX synchronization for a policy named test1, a rate limit of 23 kbps, a QoS named test, VLAN 1, and an access list named test1 under interface LAG 6:

```
switch(config)# interface lag 6
switch(config-lag-if)# vsx-sync policies rate-limits qos vlans access-lists
switch(config-lag-if)# apply policy test1 in
switch(config-lag-if)# rate-limit broadcast 23 kbps
switch(config-lag-if)# apply qos schedule-profile test
switch(config-lag-if)# vlan trunk native 1
switch(config-lag-if)# apply access-list ip test 1 in
```

Enabling VSX synchronization for a port filter:

```
switch(config)# interface 1/1/1
switch(config-if)# vsx-sync portfilter
```

```
switch(config)# interface lag 1
switch(config-lag-if)# vsx-sync portfilter
```

Enabling VSX synchronization for a PVLAN port type configuration under interface LAG 3:

```
switch(config)# interface lag 3
switch(config-lag-if)# vsx-sync private-vlan-port-type
```

Enabling VSX synchronization for DHCP snooping configuration under interface LAG 9:

```
switch(config)# interface lag 9 multi-chassis
switch(config-lag-if)# vsx-sync dhcp-snooping
```

Disabling VSX synchronization for DHCP snooping configuration under interface LAG 9:

```
switch(config)# interface lag 9 multi-chassis
switch(config-lag-if)# no vsx-sync dhcp-snooping
```

Disabling VSX synchronization for access lists and policies under logical interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no vsx-sync access-lists policies
```

Disabling VSX synchronization for access lists and policies under interface LAG 2:

```
switch(config)# interface lag 2
switch(config-if)# no vsx-sync access-lists policies
```

Enabling VSX synchronization of IRDP configurations under logical interface 1/1/1. The first five lines in the example configure IRDP and the last line enables VSX synchronization for IRDP configurations associated under interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip irdp
switch(config-if)# ip irdp minadvertinterval 550
```

```
switch(config-if)# ip irdp maxadvertinterval 850
switch(config-if)# ip irdp holdtime 900
switch(config-if)# vsx-sync irdp
```

Disabling VSX synchronization for a PVLAN port type configuration under interface LAG 8:

```
switch(config)# interface lag 8
switch(config-lag-if)# no vsx-sync private-vlan-port-type
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification                                                           |
|------------------|------------------------------------------------------------------------|
| 10.09            | Added <code>private-vlan-port-type</code> parameter. Updated examples. |
| 10.07 or earlier | --                                                                     |

## Command Information

| Platforms     | Command context                                      | Authority                                                                          |
|---------------|------------------------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-if</code><br><code>config-lag-if</code> | Administrators or local user group members with execution rights for this command. |

## vsx-sync (config-vlan-if context)

```
vsx-sync {[active-gateways] [policies]}
no vsx-sync {[active-gateways] [policies]}
```

### Description

Enables VSX sync of active gateways or policies associated under an interface. To synchronize the associations, you must configure the same `interface vlan` on the peer switch.

The **no** form of this command removes VSX synchronization for active gateways or policies associated under an interface, but it does not remove the feature configurations from the secondary peer switch.

| Parameter                                   | Description                                                                              |
|---------------------------------------------|------------------------------------------------------------------------------------------|
| <code>{[active-gateways] [policies]}</code> | Specifies one or more of the features for which to enable VSX synchronization.           |
| <code>access-gateways</code>                | Specifies that active gateways associated with an interface are enabled for VSX syncing. |
| <code>policies</code>                       | Specifies that policies associated with an interface are enabled for VSX syncing.        |

### Usage

Configure an SVI on the secondary switch; however, you do not need to run the `vsx-sync active-gateways` command on the secondary VSX switch.



Do not use peer system MAC address as an active-gateway VMAC. If same MAC address is used, the VSX synchronization will try to sync the configuration on secondary switch and cause traffic disruptions.

## Examples

Enabling VSX synchronization for an active gateway associated with VLAN 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# vsx-sync active-gateways
```

Enabling VSX synchronization for policies associated with VLAN 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# vsx-sync policies
```

Enabling VSX synchronization for active gateways and policies associated with VLAN 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# active-gateway ip 10.10.10.10 mac 23:24:25:26:27:28
switch(config-if-vlan)# active-gateway ipv6 fd12:3456:789a:1::1 mac
fd12:3456:789a:1::1 23:24:25:26:27:28
switch(config-if-vlan)# vsx-sync active-gateways policies
```

Disabling VSX synchronization for active gateways associated with VLAN 1:

```
switch(config)# interface vlan 1
switch(config-if-vlan)# no vsx-sync active-gateways
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-if-vlan  | Administrators or local user group members with execution rights for this command. |

## vsx-sync aaa

vsx-sync aaa

```
no vsx-sync aaa
```

## Description

Enables VSX synchronization of all AAA configurations, including user, RADIUS server, and TACACS+ server, on the primary VSX node to the secondary peer switch.

The **no** form of this command removes VSX synchronization of global AAA configurations, but it does not remove the existing global AAA feature configurations from the secondary peer switch.

## Examples

Enabling VSX sync for the AAA configurations to the secondary peer:

```
switch(config)# vsx
switch(config-vsx)# vsx-sync aaa
```

Disabling VSX sync for the AAA configurations to the secondary peer:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync aaa
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync acl-log-timer

```
vsx-sync acl-log-timer
no vsx-sync acl-log-timer
```

## Description

Enables VSX synchronization of access list log timer configurations on the primary VSX node to the secondary peer.

The **no** form of this command removes VSX synchronization of access list log timer configurations to the secondary peer. However, it does not remove the previously synced configurations from the secondary peer switch.

## Examples

Enabling VSX sync for the access list log timer configurations:

```
switch(config)# access-list log timer 30
switch(config)# vsx
switch(config-vsx)# vsx-sync acl-log-timer
```

Disabling VSX sync for the access list log timer configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync acl-log-timer
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync acl-secure-update

```
vsx-sync acl-secure-update
no vsx-sync acl-secure-update
```

### Description

If this setting is enabled and the primary VSX node has configurations with the access list secure-update feature enabled, this configuration can synchronize to the secondary peer. This setting is disabled by default.

The **no** form of the command disables the syncing of access list secure-update configurations to the secondary peer, but that does not remove any existing access list secure-update feature configurations from the secondary peer.

### Examples

Enabling VSX sync for configurations with the access list secure-update feature:

```
switch(config)# vsx
switch(config-vsx)# vsx-sync acl-secure-update
```

Disabling VSX sync for configurations with the access list secure-update feature:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync acl-secure-update
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Related Commands

| Command                                | Description                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>access-list secure-update</code> | This command determines if access lists are updated using the secure-update feature. Secure-update is enabled by default. Refer to the <i>ACLs and Classifiers Policy Guide</i> for details. |

## Command History

| Release | Modification        |
|---------|---------------------|
| 10.13   | -Command Introduced |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | <code>config-vsx</code> | Administrators or local user group members with execution rights for this command. |

## vsx-sync bfd-global

```
vsx-sync bfd-global
no vsx-sync bfd-global
```

### Description

Enables syncing of global BFD configurations, such as `echo-src-ip-address`, `detect-multiplier`, `min-transmit-interval`, and `min-receive-interval`, on the primary VSX node to the secondary peer.



This command enables VSX synchronization only at the top level and not at the context level.

The **no** form of this command disables the syncing of global BFD configurations to the secondary peer, but it does not remove the existing global BFD feature configurations from it.

### Examples

Enabling VSX synchronization for various global BFD configurations:

```
switch(config)# bfd detect-multiplier 1
switch(config)# bfd min-transmit-interval 1000
switch(config)# bfd min-receive-interval 1000
switch(config)# bfd echo-src-ip-address 2.2.2.2
```



```
switch(config)# bfd min-echo-receive-interval 1000
switch(config)# vsx
switch(config-vsx)# vsx-sync bfd-global
```

Disabling VSX synchronization for global BFD configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync bfd-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync bgp

```
vsx-sync bgp
no vsx-sync bgp
```

### Description

Enables syncing of BGP configurations on the primary VSX switch to the secondary peer switch.

The **no** form of this command disables syncing BGP, as path lists, community lists, prefix lists, and route map configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer switch.

### Usage

The following BGP configurations are synchronized: as path lists, community lists, prefix lists, and route map configurations. To maintain the uniqueness of a switch in the autonomous system, the BGP router ID, BGP cluster ID, and BGP neighbor update-source are not synchronized. This exclusion is required for BGP functionality to work seamlessly even with VSX topology.

Several settings are also not synced. The `neighbor <IP address> shutdown` setting is not synced because syncing that setting would cause both the primary and secondary VSX nodes towards the core to go down. In route map configurations, the following settings are also not synced from the primary VSX switch to the secondary VSX switch, because the next-hop is always set differently for the primary and secondary VSX peers:

- `set ip nexthop <IP-ADDR>`
- `set ipv6 nexthop global <IP-ADDR>`

If the next-hop must be same for both primary and secondary VSX peers, configure the same value on the individual switches.

## Examples

Enabling VSX sync for the BGP configurations:

```
switch(config)# ip aspath-list list1 seq 10 permit 10
switch(config)# ip community-list expanded com1 seq 10 permit 10
switch(config)# ip extcommunity-list standard ext1 seq 10 permit rt 10:4
switch(config)# ip prefix-list pref1 seq 10 permit any
switch(config)# route-map rml permit
switch(config-route-map-rml-10)# match ip next-hop 1.1.1.1
switch(config)# router bgp 100
switch(config-bgp)# bgp router-id 1.1.1.1
switch(config-bgp)# neighbor 12.1.1.1 remote-as 1
switch(config-bgp)# address-family ipv4 unicast
switch(config-bgp-ipv4-uc)# neighbor 12.1.1.1 activate
switch(config)# vsx
switch(config-vsx)# vsx-sync bgp
```

Disabling VSX sync for the BGP configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync bgp
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync copp-policy

```
vsx-sync copp-policy
no vsx-sync copp-policy
```

### Description

Enables VSX synchronization of CoPP policy configurations on the primary VSX node to the secondary peer switch.

The **no** form of this command removes VSX synchronization of global CoPP configurations, but it does not remove the existing global CoPP configurations from the secondary peer switch.

## Examples

The first three lines in the following example show the setting of several policy configurations. The last two lines of the example show the enabling of VSX synchronization for CoPP policy configurations.

```
switch(config)# copp-policy mypolicy
switch(config-copp)# class arp-broadcast drop
switch(config-copp)# no class arp-unicast
switch(config)# vsx
switch(config-vsx)# vsx-sync copp-policy
```

Disabling VSX synchronization for global CoPP configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync copp-policy
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync dcb-global

```
vsx-sync dcb-global
no vsx-sync dcb-global
```

### Description

Enables VSX synchronization of global DCBx configurations from the primary VSX node to the secondary peer.

The **no** form of the command disables VSX synchronization of global DCBx configurations to the secondary peer; however, it does not remove the existing DCBx feature configurations from the secondary peer.

### Usage

The following commands are synced from primary VSX node to secondary VSX node:

- `lldp dcbx`
- `dcbx application`

## Examples

The first two lines in the following example show the setting of global DCBx configurations. The last two lines in the example show the enabling of VSX synchronization for global DCBx configurations.

```
switch(config)# lldp dcbx
switch(config)# dcbx application iscsi priority 7
switch(config)# vsx
switch(config-vsx)# vsx-sync dcb-global
```

Disabling VSX synchronization for global DCBx configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync dcb-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync dhcp-relay

```
vsx-sync dhcp-relay
no vsx-sync dhcp-relay
```

### Description

Enables VSX synchronization of DHCPv4 and DHCPv6 relay configurations on the primary VSX node to the secondary peer.

The **no** form of the command disables the VSX synchronization of DHCPv4 and DHCPv6 relay configurations to the secondary peer; however, it does not remove the existing DHCPv4 and DHCPv6 relay configurations from the secondary VSX peer.

### Examples

This example enables VSX synchronization for DHCPv4 relay configurations. The first six lines in the example show DHCPv4 relay configurations. The last two lines show how to enable VSX synchronization for the DHCP relay configurations:

```
switch(config)# interface 1/1/1
switch(config-if)# ip helper-address 192.168.10.1
switch(config-if)# ip helper-address 192.168.20.1
```

```
switch(config)# interface 1/1/2
switch(config-if)# ip helper-address 192.168.30.1
switch(config)# dhcp-relay option 82
switch(config)# vsx
switch(config-vsx)# vsx-sync dhcp-relay
```

This example enables VSX synchronization for DHCPv6 relay configurations. The first seven lines in the example show DHCPv6 relay configurations. The last two lines show how to enable VSX synchronization for the DHCP relay configurations:

```
switch(config)# dhcpv6-relay
switch(config)# interface 1/1/1
switch(config-if)# ipv6 helper-address unicast 2001:db8:0:1::
switch(config-if)# ipv6 helper-address multicast FF01::1:1000 egress 1/1/2
switch(config)# interface 1/1/2
switch(config-if)# ipv6 helper-address unicast 2001:db8:0:2::
switch(config)# dhcpv6-relay option 79
switch(config)# vsx
switch(config-vsx)# vsx-sync dhcp-relay
```

Disabling VSX synchronization for DHCP relay configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync dhcp-relay
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync dhcp-server

```
vsx-sync dhcp-server
no vsx-sync dhcp-server
```

## Description

Enables VSX synchronization of all DHCPv4 server configurations, including external storage configurations, on the primary VSX node to the secondary peer. Only the primary VSX node answers DHCP service requests, and leases can only be exported from the primary VSX node.

The **no** form of the command disables VSX synchronization of DHCPv4 server configurations to the secondary peer; however, it does not remove the existing DHCPv4 server feature configurations from the secondary peer.

## Examples

The first six lines in the following example show the setting of a DHCPv4 server configuration. The last line of the example shows the enabling of VSX synchronization for global DHCPv4 server configurations.

```
switch(config)# dhcp-server external-storage dhcp-dbs file dhcpv4_lease_file delay 600
switch(config)# dhcp-server vrf default
switch(config-dhcp-server)# pool test
switch(config-dhcp-server-pool)# range 10.0.0.20 10.0.0.30
switch(config-dhcp-server-pool)# default-router 10.0.0.1 10.0.0.10
switch(config-dhcp-server-pool)# static-bind ip 10.0.0.1 mac 24:be:05:24:75:73
switch(config)# vsx
switch(config-vsx)# vsx-sync dhcp-server
```

Disabling VSX synchronization for global DHCPv4 server configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync dhcp-server
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync dhcpv6-server

```
vsx-sync dhcpv6-server
no vsx-sync dhcpv6-server
```

### Description

Enables VSX synchronization of all DHCPv6 server configurations, including external storage configurations, on the primary VSX node to the secondary peer.

The **no** form of the command disables VSX synchronization of DHCPv6 server configurations to the secondary peer; however, it does not remove the existing DHCPv6 server feature configurations from the secondary peer.

## Examples

The first six lines in the following example show the setting of a DHCPv6 server configuration. The last two lines of the example show the enabling of VSX synchronization for global DHCPv6 server configurations.

```
switch(config)# dhcpv6-server external-storage dhcpv6-dbs file dhcpv6_lease_file
delay 600
switch(config)# dhcpv6-server vrf default
switch(config-dhcp-server)# pool test
switch(config-dhcpv6-server-pool)# range 2001::1 2001::10 prefix-len 64
switch(config-dhcpv6-server-pool)# option 22 ipv6 2001::12
switch(config-dhcpv6-server-pool)# static-bind ipv6 2001::11 client-id
1:0:a0:24:ab:fb:9c
switch(config)# vsx
switch(config-vsx)# vsx-sync dhcpv6-server
```

Disabling VSX synchronization for global DHCPv6 server configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync dhcpv6-server
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync dns

```
vsx-sync dns
no vsx-sync dns
```

### Description

Enables VSX synchronization of the global DNS configurations on the primary VSX node to the secondary peer switch.

The **no** form of this command removes VSX synchronization for global DNS configurations, but it does not remove the feature configurations from the secondary peer switch.

### Examples

The first line in the following example shows the setting of a DNS configuration. The last two lines of the example show the enabling of VSX synchronization for global DNS configurations.

```
switch(config)# ip dns domain-name domain.com
switch(config)# vsx
switch(config-vsx)# vsx-sync dns
```

Disabling VSX synchronization for global DNS configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync dns
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync evpn

```
vsx-sync evpn
no vsx-sync evpn
```

### Description

Enables syncing of all EVPN context-related configurations on primary VSX node to the secondary peer switch.

The **no** form of this command disables syncing EVPN configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer switch.



As a prerequisite, VLAN vsx-sync must be enabled separately for the VLAN configurations inside EVPN context to get synced.

## Examples

Enabling VSX sync for the EVPN configurations:

```
switch(config)# vlan 2
switch(config-vlan-2)# vsx-sync
switch(config)# evpn
switch(config-evpn)# vlan 2
switch(config-evpn-vlan-2)# rd 5:5
switch(config-evpn-vlan-2)# route-target export 1:1
```



```
switch(config-evpn-vlan-2) # route-target import 1:1
switch(config) # vsx
switch(config-vsx) # vsx-sync evpn
```

Disabling VSX sync for the EVPN configurations:

```
switch(config) # vsx
switch(config-vsx) # no vsx-sync evpn
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync icmp-tcp

```
vsx-sync icmp-tcp
no vsx-sync icmp-tcp
```

### Description

Enables VSX synchronization of IP ICMP configurations, including `ip icmp unreachable`, `ip icmp redirect`, and `ip icmp throttle` configurations, on primary VSX node to the secondary peer.

The **no** form of the command disables the VSX synchronization of IP ICMP configurations to the secondary peer. However, it does not remove the existing IP ICMP configurations from the secondary VSX peer.

### Examples

Enabling VSX synchronization for IP ICMP configurations:

```
switch(config) # vsx
switch(config-vsx) # vsx-sync icmp-tcp
```

Disabling VSX synchronization for IP ICMP configurations:

```
switch(config) # vsx
switch(config-vsx) # no vsx-sync icmp-tcp
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync keychain

vsx-sync keychain  
no vsx-sync keychain

### Description

Enables synchronizing of key chain configurations on primary VSX node to the secondary peer. There is no configuration synchronization from secondary to primary peer.

If any additional modification or configuration is made on the primary for the key chain set of features, the features will be auto-synchronized.

The **no** form of the command disables synchronizing key chain configurations to the secondary peer. But it does not remove the previously synchronized configurations from the secondary peer.

### Examples

Enabling synchronizing of key chain configurations on primary VSX node to the secondary peer:

```
switch(config)# keychain ospf_keys
switch(config-keychain)# key 1
switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2019 end-time
10:10:10 11/25/2019
switch(config-keychain-key)# accept-lifetime duration infinite
switch(config)# vsx
switch(config-vsx)# vsx-sync keychain
```

Disabling synchronizing key chain configurations to the secondary peer:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync keychain
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync lldp

```
vsx-sync lldp
no vsx-sync lldp
```

### Description

Enables VSX synchronization of the LLDP configurations on the primary VSX node to the secondary peer.

The **no** form of this command disable VSX synchronization of LLDP configurations to the secondary peer, but it does not remove the existing LLDP feature configurations from the secondary peer switch.

### Examples

The first line in the following example shows the setting of an LLDP configuration. The last two lines of the example show the enabling of VSX synchronization for LLDP configurations.

```
switch(config)# lldp reinit 6
switch(config)# vsx
switch(config-vsx)# vsx-sync lldp
```

Disabling VSX synchronization of LLDP configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync lldp
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# vsx-sync loop-protect-global

```
vsx-sync loop-protect-global
no vsx-sync loop-protect-global
```

## Description

Enables the VSX synchronization of global loop protect configurations, such as transmit-interval and re-enable-timer, on the primary VSX node to the secondary peer switch. To enable VSX synchronization at the context level for this feature, enter the `vsx-sync mclag-interfaces` command at the context level. The **no** form of this command removes VSX synchronization of global loop protect configurations, but it does not remove the existing global loop protect feature configurations from the secondary peer switch.

## Examples

The first two lines in the following example show the setting of global loop protect configurations. The last two lines of the example show the enabling of VSX synchronization for global loop protect configurations.

```
switch(config)# loop-protect transmit-interval 10
switch(config)# loop-protect re-enable-timer 300
switch(config)# vsx
switch(config-vsx)# vsx-sync loop-protect-global
```

Disabling VSX synchronization of global loop protect configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync loop-protect-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# vsx-sync mclag-interfaces

```
vsx-sync mclag-interfaces
no vsx-sync mclag-interfaces
```

## Description

Enables the VSX synchronization of VSX LAG interface associations and attributes on the primary VSX switch to the secondary peer switch. The Usage section in this topic provides a listing of specific associations and attributes that are synchronized to the secondary switch.

The **no** form of this command removes VSX synchronization of global VSX LAG and attributes, but it does not remove the existing VSX LAG feature configurations from the secondary peer switch.

## Usage

The VSX LAG interface associations and attributes that support VSX synchronization are for example: Interface associations:

- Access lists
- Policies
- QoS
- Port access
- Port filters
- Rate limits
- VLANs

Supported attributes:

- LAG description
- LACP
- Loop protect
- QoS trust
- sFlow
- STP

This configuration overrides the existing VSX synchronization associations created under the VSX LAG interface context. Also with this configuration, the system blocks further configuration of VSX synchronization associations under the VSX LAG context.

## Examples

The first four lines in the following example show the creation and configuration of a VSX LAG. The last two lines of the example show the enabling of VSX synchronization for VSX LAG interface associations and attributes.

```
switch(config)# interface lag 1 multi-chassis
switch(config-lag-if)# access-list ip MY_IP_ACL in
switch(config-lag-if)# rate-limit broadcast 50 kbps
switch(config-lag-if)# qos trust cos
switch(config-lag-if)# exit
switch(config)# vsx
switch(config-vsx)# vsx-sync mclag-interfaces
```

Disabling the VSX synchronization of VSX LAG interface associations and attributes:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync mclag-interfaces
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync nd-snooping

vsx-sync nd-snooping  
no vsx-sync nd-snooping

### Description

Enables VSX synchronization of ND snooping configurations on the primary VSX node to the secondary peer switch.

To synchronize ND snooping configurations associated with a particular VLAN and interface, configure the same VLAN and interface on the peer device.

When RA guard policy is enabled, this command also synchronizes RA guard policy related configurations.

The **no** form of this command disables syncing ND snooping configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer.

### Examples

Enabling VSX sync for the ND snooping configurations to the secondary peer:

```
switch(config)# interface 1/1/3
switch(config-if)# no routing
switch(config-if)# nd-snooping trust
switch(config)# vlan 2
switch(config-vlan-2)# nd-snooping
switch(config-vlan-2)# nd-snooping ra-drop
switch(config-vlan-2)# nd-snooping prefix-list 2001::2/64
switch(config)# vsx
switch(config-vsx)# vsx-sync nd-snooping
```

Disabling VSX sync for the ND snooping configurations to the secondary peer:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync nd-snooping
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync neighbor

vsx-sync neighbor  
no vsx-sync neighbor

### Description

Enables VSX synchronization of IPv4 and IPv6 static neighbors configuration on primary VSX node to the secondary peer. There is no configuration sync from secondary to primary peer. If any new modification or additional configuration is made on the primary node for IPv4 and IPv6 static neighbors configuration, they will be auto-synced.

The **no** form of this command VSX synchronization of IPv4 and IPv6 static neighbors configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer switch.

### Examples

Enabling VSX sync for the IPv4 and IPv6 static neighbors configurations:

```
DUT-1 (config-vsx)# show run in vlan127
interface vlan127
 ip address 137.1.1.1/16
 ipv6 address 7f00::1/64
 arp ipv4 137.1.1.35 mac 00:12:01:00:00:1a
 arp ipv4 137.1.1.70 mac 00:12:01:00:00:3d
 exit
DUT-1 (config-vsx)
switch(config)# vsx
switch(config-vsx)# vsx-sync neighbor
```

Disabling VSX sync for the IPv4 and IPv6 static neighbors configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync neighbor
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync ospf

vsx-sync ospf  
no vsx-sync ospf

### Description

Enables syncing of OSPF (including OSPFv2 and OPSFv3), route map, and key chain configurations on the primary VSX switch. There is no configuration sync from secondary to primary peer.

To synchronize OSPF configurations at the port level context, configure the same port on the peer device.

The **no** form of this command disables syncing of OSPF, route map, and key chain configurations to the secondary peer. But it does not remove the previously synced configurations from the secondary peer switch.



The OSPF router ID is not synchronized. This exclusion is needed because the router ID uniquely identifies the router. The two OSPF routers with the same router ID do not form an adjacency between them.

### Examples

Enabling VSX sync for the OSPF configurations to the secondary peer:

```
switch(config)# router ospf 1
switch(config-ospf-1)# area 0
switch(config-ospf-1)# area 1 nssa
switch(config-ospf-1)# area 2 stub
switch(config-ospf-1)# redistribute connected route-map map1
switch(config)# router ospfv3 1
switch(config-ospfv3-1)# max-metric router-lsa on-startup
switch(config-ospfv3-1)# bfd all-interfaces
switch(config-if)# ip ospf 1 area 0
switch(config-if)# ip ospf hello-interval 33
switch(config-if)# ipv6 ospfv3 1 area 0
switch(config-if)# ipv6 ospfv3 dead-interval 55
switch(config)# vsx
switch(config-vsx)# vsx-sync ospf
```

Disabling VSX sync for the OSPF configurations to the secondary peer:



```
switch(config)# vsx
switch(config-vsx)# no vsx-sync ospf
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync policy-global

```
vsx-sync policy-global
no vsx-sync policy-global
```

### Description

Enables VSX synchronization of global classifier policy configurations on the primary VSX node to the secondary peer switch.

The **no** form of this command disables VSX synchronization of global policy configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer switch.

### Examples

Enabling VSX sync for the global policy configurations to the secondary peer:

```
switch(config)# apply policy testPolicy in
switch(config)# vsx
switch(config-vsx)# vsx-sync policy-global
```

Disabling VSX sync for the global policy configurations to the secondary peer:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync policy-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync qos-global

```
vsx-sync qos-global
no vsx-sync qos-global
```

### Description

Enables the VSX synchronization of global QoS configurations, such as CoS map, DSCP map, and trust policy, on the primary VSX node to the secondary peer switch. To enable VSX synchronization at the context level for this feature, enter the `vsx-sync qos` command at the context level.

The **no** form of this command removes VSX synchronization of global QoS configurations, but it does not remove the existing global QoS feature configurations from the secondary peer switch.

### Examples

The first five lines in the following example show the setting of global QoS configurations. The last two lines of the example show the enabling of VSX synchronization for global QoS configurations.

```
switch(config)# qos cos-map 1 local-priority 0
switch(config)# qos cos-map 0 local-priority 1
switch(config)# qos cos-map 2 local-priority 2
switch(config)# qos dscp-map 2 local-priority 3
switch(config)# qos trust dscp
switch(config)# vsx
switch(config-vsx)# vsx-sync qos-global
```

Disabling VSX synchronization of global QoS configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync qos-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync route-map

```
vsx-sync route-map
no vsx-sync route-map
```

### Description

Enables syncing of all As Path lists, community lists, prefix lists, and route map configurations on primary VSX node to the secondary peer switch. There is no configuration sync from the secondary to primary peer.

The **no** form of this command disables syncing of As Path lists, community lists, prefix lists, and route map configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer switch.



When vsx-sync for BGP or OSPF is configured, route map configurations are synchronized from primary VSX node to the secondary peer due to the dependency in configurations.

### Examples

Enabling VSX sync for the route map configurations:

```
switch(config)# ip aspath-list list1 seq 10 permit 10
switch(config)# ip community-list expanded com1 seq 10 permit 10
switch(config)# ip extcommunity-list standard ext1 seq 10 permit rt 10:4
switch(config)# ip prefix-list pref1 seq 10 permit any
switch(config)# route-map rml permit
switch(config-route-map-rml-10)# match ip next-hop 1.1.1.1
switch(config)# vsx
switch(config-vsx)# vsx-sync route-map
```

Disabling VSX sync for the route map configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync route-map
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync sflow

```
vsx-sync sflow
no vsx-sync sflow
```

### Description

Enables VSX synchronization of the sFlow configurations on the primary VSX node to the secondary peer.

The **no** form of this command removes VSX synchronization of global sFlow configurations, but it does not remove the existing global sFlow feature configurations from the secondary peer switch.

### Usage

To maintain compliance with sFlow collector functionality for non-VSX topology, the `vsx-sync sflow` command on primary VSX peer is expected to sync all sFlow configurations, except for the `agent-ip` configuration. This exclusion is required for sFlow collector functionality to work seamlessly even with VSX topology.

### Examples

The first line in the following example shows the setting of an sFlow configuration. The last two lines of the example show the enabling of VSX synchronization for sFlow configurations.

```
switch(config)# sflow agent-ip 10.0.0.100
switch(config)# vsx
switch(config-vsx)# vsx-sync sflow
```

Disabling VSX synchronization of global sFlow configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync sflow
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync sflow-global

```
vsx-sync sflow-global
no vsx-sync sflow-global
```

### Description

Enables VSX synchronization of the sFlow global configurations on the primary VSX node to the secondary peer.

The **no** form of this command disables VSX synchronization of global sFlow configurations, but it does not remove the existing sFlow feature configurations from the secondary peer switch.

### Usage

To maintain compliance with sFlow collector functionality for non-VSX topology, the `vsx-sync sflow` command on primary VSX peer is expected to sync all sFlow configurations, except for the `agent-ip` configuration. This exclusion is required for sFlow collector functionality to work seamlessly even with VSX topology. VSX syncs only the global sFlow configurations and not the sFlow configurations under physical or LAG interfaces.

### Examples

The first line in the following example shows the setting of an sFlow configuration. The last two lines of the example show the enabling of VSX synchronization for sFlow configurations.

```
switch(config)# sflow collector 1.1.1.1
switch(config)# vsx
switch(config-vsx)# vsx-sync sflow-global
```

Disabling VSX synchronization of global sFlow configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync sflow-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync snmp

```
vsx-sync snmp
no vsx-sync snmp
```

### Description

Enables VSX synchronization of SNMP configurations on the primary VSX node to the secondary peer. The **no** form of this command removes VSX synchronization of global SNMP configurations, but it does not remove the existing global SNMP feature configurations from the secondary peer switch.

### Examples

Enabling VSX synchronization for SNMP configuration:

```
switch(config)# vsx
switch(config-vsx)# vsx-sync snmp
```

Disabling VSX synchronization for SNMP configuration:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync snmp
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

### Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync ssh

```
vsx-sync ssh
no vsx-sync ssh
```

### Description

Enables VSX synchronization of SSH server configurations on the primary VSX node to the secondary peer switch.

The **no** form of this command removes VSX synchronization of global SSH configurations, but it does not remove the existing global SSH feature configurations from the secondary peer switch.

## Examples

The first line in the following example shows the setting of an SSH server configuration. The last two lines of the example show the enabling of VSX synchronization for SSH server configurations.

```
switch(config)# ssh certified-algorithms-only
switch(config)# vsx
switch(config-vsx)# vsx-sync ssh
```

Disabling VSX synchronization for global SSH server configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync ssh
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync static-routes

```
vsx-sync static-routes
no vsx-sync static-routes
```

## Description

Enables VSX synchronization of static route configurations on the primary VSX node to the secondary peer switch.

The **no** form of this command removes VSX synchronization of global static route configurations, but it does not remove the existing global static route feature configurations from the secondary peer switch.

## Examples

Enabling VSX synchronization for static routes:

```
switch(config)# vsx
switch(config-vsx)# vsx-sync static-routes
```

Disabling VSX synchronization for static routes:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync static-routes
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync stp-global

```
vsx-sync stp-global
no vsx-sync stp-global
```

### Description

Enables the VSX synchronization of global STP configurations on the primary VSX node to the secondary peer switch. Use the `vsx-sync mclag-interfaces` command to sync context level spanning trees. To enable VSX synchronization at the context level for this feature, enter the `vsx-sync mclag-interfaces` command at the context level.

The **no** form of this command removes VSX synchronization of global STP configurations, but it does not remove the existing global STP feature configurations from the secondary peer switch.

### Examples

The first two lines in the following example show the setting of global STP configurations. The last two lines of the example show the enabling of VSX synchronization for global STP configurations.

```
switch(config)# spanning-tree config-name abc
switch(config)# spanning-tree config-revision 1
switch(config)# vsx
switch(config-vsx)# vsx-sync stp-global
```

Disabling VSX synchronization of global STP configurations:



```
switch(config)# vsx
switch(config-vsx)# no vsx-sync stp-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# vsx-sync telnet

vsx-sync telnet  
no vsx-sync telnet

## Description

Enables VSX synchronization of Telnet server configurations from the primary VSX node to the secondary peer. To synchronize Telnet configurations associated with a particular VRF, you need to configure the same VRF on the peer device.

The **no** form of the command disables VSX synchronization of Telnet server configurations to the secondary peer, however, it does not remove the existing Telnet server configurations from the secondary peer.

## Examples

Enabling VSX synchronization of Telnet servers:

```
switch(config)# telnet server vrf main
switch(config)# vsx
switch(config-vsx)# vsx-sync telnet
```

Disabling VSX synchronization of Telnet servers:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync telnet
```

## Command History

| Release | Modification                                                                 |
|---------|------------------------------------------------------------------------------|
| 10.11   | Command introduced on the 8320, 8325, 8360, 8400, 9300, 10000 Switch series. |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

# vsx-sync time

vsx-sync time  
no vsx-sync time

## Description

Enables VSX synchronization of time-related configurations, including NTP and time zone configurations, on the primary VSX node on the secondary peer switch.

The **no** form of this command removes VSX synchronization of global time-related configurations, but it does not remove the existing global time-related feature configurations from the secondary peer switch.

## Examples

The first two lines in the following example show the setting of time-related configurations. The last two lines of the example show the enabling of VSX synchronization for time-related configurations.

```
switch(config)# ntp authentication
switch(config)# clock timezone utc
switch(config)# vsx
switch(config-vsx)# vsx-sync time
```

Disabling VSX synchronization for time-related configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync time
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync udp-forwarder

```
vsx-sync udp-forwarder
no vsx-sync udp-forwarder
```

### Description

Enables VSX synchronization of UDP forwarder configurations on the primary VSX node to the secondary peer.

The **no** form of the command disables the VSX synchronization of UDP forwarder configurations to the secondary peer; however, it does not remove the existing udp-forwarder configurations from the secondary VSX peer.

### Examples

Enabling VSX synchronization for UDP forwarder configurations:

```
switch(config)# vsx
switch(config-vsx)# vsx-sync udp-forwarder
```

Disabling VSX synchronization for UDP forwarder configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync udp-forwarder
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync vrrp

```
vsx-sync vrrp
no vsx-sync vrrp
```

### Description

Enables VSX synchronization of all VRRP configurations on the primary VSX node to the secondary peer switch. There is no configuration sync from secondary to primary peer.

To synchronize VRRP configurations at the port level context, the same port must be configured on the peer device with IP address.

The **no** form of this command disables syncing VRRP configurations to the secondary peer, but it does not remove the previously synced configurations from the secondary peer.

BFD IP is the IP address of VRRP peer device. Hence it cannot be synced.



In the owner scenario, in case the priority is synced, both VSX primary and secondary devices will have 255 as their priority. If the primary device goes down and comes up again, the secondary device will still act as the Active in spite of the primary device being the owner. Hence priority cannot be synced.

## Examples

Enabling VSX sync for the VRRP configurations to the secondary peer:

```

switch(config)# router vrrp enable
switch(config-if)# vrrp 1 address-family ipv4
switch(config-if-vrrp)# address 1.1.1.100 primary
switch(config-if-vrrp)# timers advertise 1000
switch(config-if-vrrp)# no shutdown
switch(config-if)# vrr 1 address-family ipv6
switch(config)# vsx
switch(config-vsx)# vsx-sync vrrp

```

Disabling VSX sync for the VRRP configurations to the secondary peer:

```
switch(config)#
```

```
switch(config-vsx)# no vsx-sync vrrp
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx-sync vsx-global

```

vsx-sync vsx-global
no vsx-sync vsx-global

```

## Description

Enables VSX synchronization of global VSX configurations on the primary VSX node to the secondary peer.

The **no** form of the command disables VSX synchronization of global VSX configurations to the secondary peer; however, it does not remove the existing VSX feature configurations from the secondary peer.

## Usage

The following commands are synced from primary VSX node to secondary VSX node:

- `inter-switch-link dead-interval <DEAD-INTERVAL>`
- `inter-switch-link hello-interval <HELLO-INTERVAL>`
- `inter-switch-link hold-time <HOLD-INTERVAL>`
- `inter-switch-link peer-detect-interval <PEER-DETECT-INTERVAL>`
- `keepalive dead-interval <DEAD-INTERVAL>`
- `keepalive hello-interval <HELLO-INTERVAL>`
- `keepalive udp-port <PORT-NUM>`
- `linkup-delay-timer <DELAY-TIMER>`
- `split-recovery`
- `system-mac <MAC-ADDR>`

## Examples

The first three lines in the following example show the setting of global VSX configurations. The last line in the example shows the enabling of VSX synchronization for global VSX configurations.

```
switch(config)# vsx
switch(config-vsx)# inter-switch-link dead-interval 15
switch(config-vsx)# inter-switch-link hello-interval 2
switch(config-vsx)# inter-switch-link hold-time 1
switch(config-vsx)# vsx-sync vsx-global
```

Disabling VSX synchronization for global VSX configurations:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync vsx-global
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vsx      | Administrators or local user group members with execution rights for this command. |

## vsx update-software

`vsx update-software <REMOTE-URL> [vrf <VRF-NAME>]`

### Description

This command lets you update the software.

| Parameter                         | Description                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;REMOTE-URL&gt;</code>   | Specifies the TFTP URL for downloading the software. Syntax:<br>tftp://{<IP-ADDRESS> <HOSTNAME>}[:<PORT>]<br>[;blocksize=<VAL>]/<FILE-NAME> |
| <code>vrf &lt;VRF-NAME&gt;</code> | Specifies the VRF name for downloading the software. Optional                                                                               |

## Usage

This command gives you the option to save the running configuration on the primary and secondary VSX switches. After the command saves the running configuration, it downloads new software from the TFTP server and verifies the download. After a successful verification, the command installs the software to the alternative image of both the VSX primary and secondary switches.

The command displays the status of the VSX primary and secondary switches during the upgrade. The command also refreshes the progress bar as the image update progresses. Do not interrupt the VSX primary CLI session until the software updates completes; however, software update process can be stopped. If you stop the upgrade when the secondary switch has already installed the image in its flash memory or the secondary switch has started the reboot the process, it comes up with the new software. The primary switch continues to have with older software. You can stop the software update process by pressing **ctrl+c**.

## Example

Updating the software using TFTP:

```
switch# vsx update-software tftp://192.168.1.1/XL.10.0x.xxxx vrf mgmt
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

This command will download new software to the %s image of both the VSX primary
and
secondary systems, then reboot them in sequence. The VSX secondary will reboot
first, followed by the primary.
Continue (y/n)? y
VSX Primary Software Update Status : <VSX primary software update status>
VSX Secondary Software Update Status : <VSX secondary software update status>
VSX ISL Status : <VSX ISL status>
Progress
[.....]
Secondary VSX system updated completely. Rebooting primary.
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

## vsx update-software boot-bank

`vsx update-software boot-bank {primary | secondary}`

### Description

Upgrades the VSX pairs using the specified bank on both the devices. This command compares whether the image versions are same in both the primary and secondary switches and reboots them in sequence, the VSX secondary switch followed by VSX primary switch.



Before executing this command, download the software image and install in the required boot banks.

| Parameter                          | Description                                                              |
|------------------------------------|--------------------------------------------------------------------------|
| <code>boot-bank</code>             | Specifies the boot bank where the image is pre-staged .                  |
| <code>{primary   secondary}</code> | Selects either primary or secondary VSX switch for the software upgrade. |

### Usage

This command gives you the option to save the running configuration on the primary and secondary VSX switches. After the command saves the running configuration, it downloads new software from the TFTP server and verifies the download. After a successful verification, the command installs the software to the alternative image of both the VSX primary and secondary switches.

The command displays the status of the VSX primary and secondary switches during the upgrade. The command also refreshes the progress bar as the image update progresses. Do not interrupt the VSX primary CLI session until the software updates completes; however, software update process can be stopped. If you stop the upgrade when the secondary switch has already installed the image in its flash memory or the secondary switch has started the reboot the process, it comes up with the new software. The primary switch continues to have with older software. You can stop the software update process by pressing **ctrl+c**.

### Example

Selecting primary bank for upgrade:

```
switch# vsx update-software boot-bank primary
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

This command will upgrade both VSX primary and secondary systems, using pre-staged
image 'X' installed in secondary bank on both devices, then reboot
them in sequence. The VSX secondary will reboot first, followed by primary.
Continue (y/n)? y
VSX Primary Software Update Status : Reboot started
VSX Secondary Software Update Status : Image updated successfully
VSX ISL Status : Up
```



```
Progress [.....]
Secondary VSX system updated completely. Rebooting primary.
```

Selecting secondary bank for upgrade:

```
switch# vsx update-software boot-bank secondary
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

This command will upgrade both VSX primary and secondary systems, using pre-staged
image 'X' installed in secondary bank on both devices, then reboot
them in sequence. The VSX secondary will reboot first, followed by primary.
Continue (y/n)? y
VSX Primary Software Update Status : Reboot started
VSX Secondary Software Update Status : Image updated successfully
VSX ISL Status : Up
Progress [.....]
Secondary VSX system updated completely. Rebooting primary.
```



For more information on features that use this command, refer to the VSX Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Administrators or local user group members with execution rights for this command. |

### interface vxlan

```
interface vxlan 1 [mode ipv4|ipv6]
no interface vxlan 1 [mode ipv4|ipv6]
```

#### Description

Creates VXLAN interface 1 and changes to the **config-vxlan-if** context. A maximum of one VXLAN interface is supported. By default, the VXLAN is disabled. To enable the VXLAN, use the command **no shutdown**.

The **no** form of this command removes VXLAN interface 1. This deletes the VXLAN tunnel, and all VNIs and VLAN-to-VNI mappings associated with it.

| Parameter      | Description                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 1              | Only one VXLAN interface is supported.                                                                                                     |
| mode ipv4 ipv6 | (Optional) Specify if the interface tunnel uses IPv4 or IPv6 addressing. If this parameter is not included, the interface default is IPv6. |

#### Examples

Creating VXLAN interface 1:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)#
```

Deleting VXLAN interface 1:

```
switch(config)# no interface vxlan 1
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

#### Command History

| Release          | Modification                                                     |
|------------------|------------------------------------------------------------------|
| 10.11.1000       | Added IPv6 support for 6300, 6400, 8100, and 8360 Switch Series. |
| 10.07 or earlier | --                                                               |

#### Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config          | Administrators or local user group members with execution rights for this command. |

## routing

```
vni <VNI-NUMBER>
no vni <VNI-NUMBER>
```

### Description

Enables a layer 3 VNI for EVPN VXLAN distributed L3 gateways with symmetric IRB. The VNI is automatically assigned the default VRF. To assign another VRF, use the command **vrf**. Used with EVPN-based VXLANs.

If a user attempts to disable routing for a VNI that has a policy or ACL applied, or tries to enable routing on a VNI already associated with a VLAN, an appropriate error or warning message is displayed to prevent potential configuration conflicts.

The **no** form of this command disables symmetric routing on a VNI.



If you enable this configuration, collection of flow tracking statistics is disabled.

### Examples

Enabling L3 VNI **1000** for EVPN VXLAN distributed L3 gateways with symmetric IRB using VRF **vrf-1**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# routing
switch(config-vni-1000)# vrf vrf-1
```

Disabling L3 VNI **1000** for EVPN VXLAN distributed L3 gateways with symmetric IRB:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# no routing
```

Trying to disable routing on VNI while ACL is applied:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 4000
switch(config-vni-1000)# vrf red
switch(config-vni-1000)# routing
switch(config-vni-1000)# apply access-list myACL routed-in
switch(config-vni-1000)# no routing
Cannot disable routing on VNI while ACL is applied. Remove ACL from VNI 4000 to proceed.
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification                                                                                          |
|------------------|-------------------------------------------------------------------------------------------------------|
| 10.17            | Added information regarding the process of disabling routing for a VNI with an applied policy or ACL. |
| 10.14            | Added information related to role based IPFIX.                                                        |
| 10.07 or earlier | --                                                                                                    |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vni-<VNI-NUMBER> | Administrators or local user group members with execution rights for this command. |

## show interface vxlan

show interface vxlan <IFNAME>

### Description

Shows detailed VXLAN interface information.

| Parameter | Description                            |
|-----------|----------------------------------------|
| <IFNAME>  | Specifies the VXLAN interface to show. |

### Example

Showing settings for VXLAN interface 1.

```
switch# show interface vxlan1
Interface vxlan1 is up
Admin state is up
Description:VXLAN1
Underlay VRF: default
Destination UDP port: 4789
VTEP source IPv4 address: 1.1.1.1
```

| VNI  | Routing  | VLAN | VRF     | VTEP Peers | Origin |
|------|----------|------|---------|------------|--------|
| 10   | disabled | 10   | --      | 2.2.2.2    | static |
| 10   | disabled | 10   | --      | 3.3.3.3    | static |
| 10   | disabled | 10   | --      | 4.4.4.4    | static |
| 20   | disabled | 20   | --      | 5.5.5.5    | evpn   |
| 20   | disabled | 20   | --      | 6.6.6.6    | evpn   |
| 30   | disabled | --   | --      | --         | static |
| 40   | disabled | 40   | --      | --         | static |
| 50   | disabled | --   | --      | 7.7.7.7    | static |
| 4000 | enabled  | --   | default | 22.1.1.2   | evpn   |
| 4001 | enabled  | --   | default | 23.1.1.3   | evpn   |

Aggregate Statistics

```

Decap:
 104222 input packets 15841744 bytes
 236 broadcast packets 26942 bytes
 0 drop packets
Encap:
 108527 output packets 11068728 bytes
 6 BUM packets 422 bytes
 0 drop packets
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show interface vxlan multipoint-tunnel

show interface vxlan multipoint-tunnel [forwarding-status|flood-status|brief|statistics|<IP-ADDR>|brief|group-mapping]

## Description

Shows detailed VXLAN interface information.

| Parameter         | Description                                                |
|-------------------|------------------------------------------------------------|
| forwarding-status | Shows multipoint tunnel encap and decap forwarding status. |
| flood-status      | Shows multipoint tunnel flood status.                      |
| statistics        | Shows multipoint tunnel encap and decap statistics.        |
| <IP-ADDR>         | Specifies a multipoint tunnel.                             |
| brief             | Shows brief information about multipoint tunnels.          |
| group-mapping     | Shows the underlay-mapped multicast group                  |

## Example

Showing information for all multipoint tunnels:

```
switch# show interface vxlan multipoint-tunnel
```

```
Destination : 239.1.0.1
Source : 1.1.1.1
Origin : pim-bidir
VRF : default
Type : flood
Encap Status : Up
Decap Status : Up
Underlay Information
=====
```

```
 L3 Interface L2 Interface

 VLAN10 1/1/53
```

```
Destination : 239.1.0.2
Source : 1.1.1.1
Origin : pim-bidir
VRF : default
Type : flood
Encap Status : Up
Decap Status : Up
Underlay Information
=====
```

```
 L3 Interface L2 Interface

 VLAN10 1/1/53
```



The output of this command will show that multipoint-tunnels between the RP/spines and the VSX secondary leaf are not created, and that only the VSX primary is intended to forward Multicast BUM replication.

Showing brief information about multipoint tunnels with pim-bidir:

```
switch# show interface vxlan multipoint-tunnel brief
```

| Type  | Source  | Destination | Origin    | VNI | VLAN | VRF     |
|-------|---------|-------------|-----------|-----|------|---------|
| flood | 1.1.1.1 | 239.1.0.1   | pim-bidir | 1   | 1    | Default |

Showing multipoint tunnel encap and decap forwarding status:

```
switch# show interface vxlan multipoint-tunnel forwarding-status
```

| Tunnel ID | L3 Interface | Type             | Source   | Destination |
|-----------|--------------|------------------|----------|-------------|
| 3         | 1/1/51       | flood            | 5.5.5.50 | 239.1.0.0   |
| 263       | 1/1/51       | multicast-router | 5.5.5.50 | 239.1.1.0   |
| 518       | 1/1/51       | multicast-group  | 5.5.5.50 | 239.1.4.1   |
| 1         | 1/1/51       | flood            | 6.6.6.1  | 239.1.0.0   |
| 2         | 1/1/52       | flood            | 6.6.6.2  | 239.1.0.0   |

```
Status (Encap) Status (Decap)
```

| Status (Encap) | Status (Decap) |
|----------------|----------------|
| up             | NA             |
| up             | NA             |
| up             | NA             |
| NA             | up             |
| NA             | up             |

Showing multipoint tunnel flood status:

```
switch# show interface vxlan multipoint-tunnel flood-status
Tunnel ID Source Destination Status VNI VLAN

3 5.5.5.50 239.1.0.0 enabled 701 101
3 5.5.5.50 239.1.0.0 enabled 702 102
3 5.5.5.50 239.1.0.0 enabled 703 103
3 5.5.5.50 239.1.0.0 enabled 704 104
3 5.5.5.50 239.1.0.0 enabled 705 105
3 5.5.5.50 239.1.0.0 enabled 706 106
3 5.5.5.50 239.1.0.0 enabled 707 107
3 5.5.5.50 239.1.0.0 enabled 708 108
3 5.5.5.50 239.1.0.0 enabled 709 109
```

Showing multipoint tunnel encap and decap statistics:

```
switch# show interface vxlan multipoint-tunnel statistics
Tunnel ID L3 Interface Type Destination Tx Packets (Encap)

3 1/1/51 flood 239.1.0.0 11155937
263 1/1/51 multicast-router 239.1.1.0 17362368

518 1/1/51 multicast-group 239.1.4.1 17339053
1 1/1/51 flood 239.1.0.0 NA
2 1/1/52 flood 239.1.0.0 NA

Tx Bytes (Encap) Rx Packets (Decap) Rx Bytes (Decap)

9474898748 NA NA
18404110080 NA NA
18379396180 NA NA
NA 1252054 117398630
NA 11057664 9437722132
```

Showing information for multipoint tunnel (pim-bidir) with a destination IP of **239.1.0.1**:

```
switch# show interface vxlan multipoint-tunnel 239.1.0.1
Destination : 239.1.0.1
Source : 1.1.1.1
Origin : pim-bidir
VRF : default
Type : flood
Encap Status : Up
Decap Status : Up
Underlay Information
=====
L3 Interface L2 Interface

VLAN10 1/1/53
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release | Modification |
|---------|--------------|
|---------|--------------|

|                  |    |
|------------------|----|
| 10.07 or earlier | -- |
|------------------|----|

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## show interface vxlan vni

```
show interface vxlan vni <VNI-NUMBER> vteps
```

### Description

Shows detailed VNI information for VXLAN interface 1.

| Parameter    | Description                                           |
|--------------|-------------------------------------------------------|
| <VNI-NUMBER> | Specifies the number for a VNI. Range: 1 to 16777214. |

### Usage

Status can be one of the following:

- operational: Virtual network ID is fully programmed on the switch hardware.
- configuration\_error: Virtual network ID programming in the switch hardware failed due to misconfiguration.
- no\_hw\_resources: Virtual network ID programming failed in the switch hardware due to insufficient resources.
- activating: Initial state of virtual network ID when it is configured.

When a tunnel endpoint is a directly connected via nexthop, then nexthop reachability appears empty (-).

### Example

Showing VNI information:

```
switch# show interface vxlan vni
VNI : 1000 VLAN : 10
Routing : disabled VRF : --
VNI-Status : operational

VNI : 2000 VLAN : 20
Routing : enabled VRF : default
VNI-Status : activating
...
...

switch# show interface vxlan vni 1000
VNI : 1000 VLAN : 10
Routing : disabled VRF : --
VNI-Status : operational
```



```

switch# show interface vxlan vni vteps
VNI : 1000 VLAN : 10
Routing : disabled VRF : --
VNI-Status : operational
VTEPS
=====
 ORIGIN SOURCE DESTINATION VRF VTEP-STATUS

 static 11.0.0.1 11.0.0.2 default operational

VNI : 2000 VLAN : 20
Routing : enabled VRF : default
VNI-Status : operational
VTEPS
=====
 ORIGIN SOURCE DESTINATION VRF VTEP-STATUS

 evpn 11.0.0.1 14.0.0.2 default activating

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# show interface vxlan vteps

show interface vxlan vteps [detail | <IP-ADDR>]

## Description

Displays detailed VTEP information for the VXLAN interface. VTEP states can be one of the following:

- **operational:** Tunnel endpoint is fully programmed on the switch hardware.
- **configuration\_error:** Tunnel endpoint programming in the switch hardware failed due to misconfiguration.
- **no\_hw\_resources:** Tunnel endpoint programming failed in the switch hardware due to insufficient resources.
- **activating:** Initial state of tunnel endpoint when it is configured.

When a tunnel endpoint is a directly connected via nexthop, then nexthop reachability appears empty (-).

| Parameter   | Description                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------|
| detail      | Show detail VTEP information.                                                                                |
| <IPv4-ADDR> | Specifies the IP address of a VTEP peer in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255. |

## Examples

Showing information for VTEPs on a VXLAN interface with IPv4 source and destination IP addresses.

```
switch# show interface vxlan vteps
Source Destination Origin Status VNI Routing VLAN VRF

11.0.0.1 11.0.0.2 static operational 1000 disabled 10 --
11.0.0.1 12.0.0.2 static activating 2000 disabled 20 --
11.0.0.1 22.1.1.1 evpn operational 4000 enabled -- red
11.0.0.1 23.1.1.1 evpn activating 4001 enabled -- blue
```

Showing information the VTEPs on a VXLAN interface with IPv6 source and destination IP addresses.

```
switch# show interface vxlan vteps
Source Destination Origin Status VNI Routing VLAN VRF

1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1002002 disabled 2002
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1002002 disabled 2002
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1001002 disabled 1002
--
```

```

1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1002002 disabled 2002
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1002002 disabled 2002
--
Source Destination Origin Status VNI Routing VLAN
VRF

1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::5 evpn operational 1002002 disabled 2002
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::2 evpn operational 1002002 disabled 2002
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1001001 disabled 1001
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::3 evpn operational 1002002 disabled 2002
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 11 enabled --
vrf1
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 12 enabled --
vrf2
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1001001 disabled 1001
--

```

```

1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1001002 disabled 1002
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1002001 disabled 2001
--
1920:1680:1:1::1 1920:1680:1:1::4 evpn operational 1002002 disabled 2002
--

```

Showing information for VTEPs on a VXLAN interface with IPv4 source and destination addresses.

```

switch# show interface vxlan vteps 33.33.33.1
Destination : 33.33.33.1
Source : 21.21.21.1
Origin : evpn
VRF : default
Status : operational
Nexthops
=====
 IP-ADDRESS INTERFACE NEXTHOP-MAC
 -
 2.2.3.1 1/1/1 11:11:11:11:44:11
 2.2.2.1 lag1 11:11:11:11:22:11
 2.2.1.1 vlan21 11:11:11:11:11:11IP

```

```

switch# show interface vxlan vteps detail
Destination : 3.3.3.3
Source : 2.2.2.2
Origin : evpn
VRF : default
Status : operational
BcastGrpID-Configured : NA
BcastGrpID-DataPlane : 1
Nexthops
=====
 IP-ADDRESS INTERFACE NEXTHOP-MAC
 -
 11.1.1.1 1/1/1.100 38:21:c7:5c:80:80

```

Showing detailed information for VTEPs on a VXLAN interface with IPv6 source and destination addresses.

```

switch# show interface vxlan 1

Interface vxlan1 is up
Admin state is up
Description:
Underlay VRF: default
Destination UDP port: 4789
VTEP source IPv4 address:
VTEP source IPv6 address: 1920:1680:1:1::1
Inter vxlan bridging mode: deny

VNI Routing VLAN VRF VTEP Peers Origin

11 enabled -- vrf1 1920:1680:1:1::5 evpn
11 enabled -- vrf1 1920:1680:1:1::2 evpn
11 enabled -- vrf1 1920:1680:1:1::3 evpn

```

```

11 enabled -- vrf1 1920:1680:1:1::4 evpn
12 enabled -- vrf2 1920:1680:1:1::5 evpn
12 enabled -- vrf2 1920:1680:1:1::2 evpn
12 enabled -- vrf2 1920:1680:1:1::3 evpn
12 enabled -- vrf2 1920:1680:1:1::4 evpn
1001001 disabled 1001 -- 1920:1680:1:1::5 evpn
1001001 disabled 1001 -- 1920:1680:1:1::2 evpn
1001001 disabled 1001 -- 1920:1680:1:1::3 evpn
1001001 disabled 1001 -- 1920:1680:1:1::4 evpn
1001002 disabled 1002 -- 1920:1680:1:1::5 evpn
1001002 disabled 1002 -- 1920:1680:1:1::2 evpn
1001002 disabled 1002 -- 1920:1680:1:1::3 evpn
1001002 disabled 1002 -- 1920:1680:1:1::4 evpn
1002001 disabled 2001 -- 1920:1680:1:1::5 evpn
1002001 disabled 2001 -- 1920:1680:1:1::2 evpn
1002001 disabled 2001 -- 1920:1680:1:1::3 evpn
1002001 disabled 2001 -- 1920:1680:1:1::4 evpn
1002002 disabled 2002 -- 1920:1680:1:1::5 evpn
1002002 disabled 2002 -- 1920:1680:1:1::2 evpn
1002002 disabled 2002 -- 1920:1680:1:1::3 evpn
1002002 disabled 2002 -- 1920:1680:1:1::4 evpn

```

#### Aggregate Statistics

```

Decap:
35032601994 input packets 24261116182550 bytes
Encap:
68424228547 output packets 47087902492031 bytes
switch# show interface vxlan 1

```

```

Interface vxlan1 is up
Admin state is up
Description:
Underlay VRF: default
Destination UDP port: 4789
VTEP source IPv4 address:
VTEP source IPv6 address: 1920:1680:1:1::1
Inter vxlan bridging mode: deny

```

| VNI     | Routing  | VLAN | VRF  | VTEP Peers       | Origin |
|---------|----------|------|------|------------------|--------|
| 11      | enabled  | --   | vrf1 | 1920:1680:1:1::5 | evpn   |
| 11      | enabled  | --   | vrf1 | 1920:1680:1:1::2 | evpn   |
| 11      | enabled  | --   | vrf1 | 1920:1680:1:1::3 | evpn   |
| 11      | enabled  | --   | vrf1 | 1920:1680:1:1::4 | evpn   |
| 12      | enabled  | --   | vrf2 | 1920:1680:1:1::5 | evpn   |
| 12      | enabled  | --   | vrf2 | 1920:1680:1:1::2 | evpn   |
| 12      | enabled  | --   | vrf2 | 1920:1680:1:1::3 | evpn   |
| 12      | enabled  | --   | vrf2 | 1920:1680:1:1::4 | evpn   |
| 1001001 | disabled | 1001 | --   | 1920:1680:1:1::5 | evpn   |
| 1001001 | disabled | 1001 | --   | 1920:1680:1:1::2 | evpn   |
| 1001001 | disabled | 1001 | --   | 1920:1680:1:1::3 | evpn   |
| 1001001 | disabled | 1001 | --   | 1920:1680:1:1::4 | evpn   |
| 1001002 | disabled | 1002 | --   | 1920:1680:1:1::5 | evpn   |
| 1001002 | disabled | 1002 | --   | 1920:1680:1:1::2 | evpn   |
| 1001002 | disabled | 1002 | --   | 1920:1680:1:1::3 | evpn   |
| 1001002 | disabled | 1002 | --   | 1920:1680:1:1::4 | evpn   |
| 1002001 | disabled | 2001 | --   | 1920:1680:1:1::5 | evpn   |
| 1002001 | disabled | 2001 | --   | 1920:1680:1:1::2 | evpn   |
| 1002001 | disabled | 2001 | --   | 1920:1680:1:1::3 | evpn   |
| 1002001 | disabled | 2001 | --   | 1920:1680:1:1::4 | evpn   |

```

1002002 disabled 2002 -- 1920:1680:1:1::5 evpn
1002002 disabled 2002 -- 1920:1680:1:1::2 evpn
1002002 disabled 2002 -- 1920:1680:1:1::3 evpn
1002002 disabled 2002 -- 1920:1680:1:1::4 evpn

```

#### Aggregate Statistics

-----

```

Decap:
35032601994 input packets 24261116182550 bytes
Encap:
68424228547 output packets 47087902492031 bytes

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | Manager (#)     | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

# shutdown

```

shutdown
no shutdown

```

## Description

Disables the VXLAN interface and deletes all VXLAN tunnels, segments, and members on the interface. The **no** form of this command starts the VXLAN interface and creates all VXLAN tunnels and segments. If members are configured, they are added to the VXLAN segment.

## Examples

Disabling VXLAN interface 1:

```

switch(config)# interface vxlan 1 mode ipv4
switch(config-vxlan-if)# shutdown

```

Enabling VXLAN interface 1:

```

switch(config)# interface vxlan 1 mode ipv4
switch(config-vxlan-if)# no shutdown

```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vxlan-if | Administrators or local user group members with execution rights for this command. |

## source ip

source ip <IPv4-ADDR>

### Description

Configures the source IPv4 address for a VXLAN interface. All VXLAN encapsulated packets use this source IP address in the outer IP header.

If you change an existing source IP address, all tunnels with the old source IP address are deleted, and new tunnels are created with the new source IP address.

The **no** form of this command deletes the source IP address for the VXLAN interface and deletes all VXLAN tunnels using this source IP address.

| Parameter   | Description                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <IPv4-ADDR> | Specifies the IP address to assign to the VXLAN interface in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. This must be an address assigned to an existing switch interface, either a loopback interface or a layer 3 interface. |

## Examples

Configuring the loopback IP address as the source IPv4 address:

```
switch(config)# interface loopback 1
switch(config-loopback-if)# ip address 1.1.1.1/24
switch(config)# interface vxlan 1
switch# source ip 1.1.1.1
```

Configuring a layer 3 interface IP address as the source IPv4 address:

```
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# routing (6300/6400 only)
switch(config-if)# ip address 11.10.10.1/24
```

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# source ip 10.10.10.1
```

Deleting the source IP address for VXLAN interface 1:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# no source ip 10.10.10.1
```



Whenever the VxLAN source IP address or virtual MAC address is changed via the command-line interface or REST API, all the EVPN routes need to be re-advertised with new IP addresses or MAC address. Therefore, the **clear bgp** command is issued internally for all EVPN neighbors to ensure all EVPN routes get re-advertised.



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification                             |
|------------------|------------------------------------------|
| 10.11.1000       | The <IPV6-ADDR> parameter is introduced. |
| 10.07 or earlier | --                                       |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vxlan-if | Administrators or local user group members with execution rights for this command. |

## vlan

```
vlan <VLAN-ID>
no vlan <VLAN-ID>
```

### Description

Associates an existing VLAN with a VNI. Only one VLAN can be associated with a VNI and the VNI must have symmetric routing disabled. To change the VLAN associated with a VNI, execute the command **vlan** with a different VLAN ID.

The **no** form of this command removes the specified VLAN from a VNI. Traffic on the specified VLAN is no longer bridged on the VXLAN interface.

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| <VLAN-ID> | Specifies the number of an existing VLAN. Range: 2 to 4040. |

### Examples

Assigning VLAN **10** to VNI **1000**:



```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# vlan 10
```

Deleting VLAN **10** from VNI **1000**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# no vlan 10
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vni-<VNI-NUMBER> | Administrators or local user group members with execution rights for this command. |

## vni

```
vni <VNI-NUMBER>
no vni <VNI-NUMBER>
```

## Description

Creates a VNI (Virtual Network Identifier) for the VXLAN interface and changes to the `config-vni-<VNI-NUMBER>` context. The VNI identifies a VXLAN segment, which acts as a logical network. The VNI can be associated with either a VLAN or VRF.

- When the VNI is associated with a VLAN, the VNI supports asymmetric routing.
- Enable support for asymmetric routing by executing the `routing` command. By default, the VNI is associated with the default VRF. To use another VRF, execute the `vrf` command.

The **no** form of this command deletes the specified VNI from the VXLAN interface. All VXLAN tunnels, VXLAN segments, and members associated with the VNI are deleted.

| Parameter    | Description                                           |
|--------------|-------------------------------------------------------|
| <VNI-NUMBER> | Specifies the number for a VNI. Range: 1 to 16777214. |

## Examples

Creating VNI **1000**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)#
```

Deleting VNI **1000**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# no vni 1000
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vxlan-if | Administrators or local user group members with execution rights for this command. |

## vrf

```
vrf <VRF-NAME>
no vrf <VRF-NAME>
```

## Description

Changes the VRF associated with an L3 VNI after symmetric routing is activated using the `routing` command. The default VRF should not be configured as an EVPN-enabled VRF. If user tries to configure VRF on a VNI that is already associated with a VLAN, an appropriate error is displayed

If a user tries to remove or reconfigure the VRF attached to a VNI while a policy is applied, an appropriate error is displayed.

The **no** form of this command sets the VRF associated with an L3 VNI to the default VRF.

| Parameter  | Description            |
|------------|------------------------|
| <VRF-NAME> | Configure VRF for VNI. |

## Examples

Enabling L3 VNI **1000** using VRF **vrf-1**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# routing
switch(config-vni-1000)# vrf vrf-1
```

Setting the VRF on L3 VNI **1000** to the default VRF:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# routing
switch(config-vni-1000)# no vrf vrf-1
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification        |
|------------------|---------------------|
| 10.07 or earlier | Command introduced. |

## Command Information

| Platforms     | Command context                       | Authority                                                                          |
|---------------|---------------------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vni- <i>&lt;VNI-NUMBER&gt;</i> | Administrators or local user group members with execution rights for this command. |

## vtep-peer

```
vtep-peer <IPV4-ADDR>
no vtep-peer <IPV4-ADDR>
```

### Description

Adds a VTEP peer to a VNI. The VNI must not have routing enabled. The VTEP peer IP address must be reachable for a VXLAN tunnel to be established.

The **no** form of this command removes a VTEP peer from a VNI, which deletes the VXLAN tunnel to the peer.

| Parameter                | Description                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;IPV4-ADDR&gt;</i> | Specifies the IP address of a VTEP peer in IPv4 format ( <b>x.x.x.x</b> ), where <b>x</b> is a decimal number from 0 to 255. |

## Examples

Adding VTEP peer **10.10.10.1** to VNI **1000**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# vlan 10
switch(config-vni-1000)# vtep-peer 10.10.10.1
```

Deleting VTEP peer **10.10.10.1** from VNI **1000**:

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vni 1000
switch(config-vni-1000)# no vtep-peer 10.10.10.1
```



For more information on features that use this command, refer to the VXLAN Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context         | Authority                                                                          |
|---------------|-------------------------|------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vni-<VNI-NUMBER> | Administrators or local user group members with execution rights for this command. |

## vxlan-counters aggregate

*Supported on the HPE Aruba Networking 8325, 8100, 8360, 9300, 10000 Switch Series only.*

```
vxlan-counters aggregate
no vxlan-counters aggregate
```

### Description

Attaches VXLAN counters to a VXLAN interface. The counters aggregate statistics for packets sent through the interface. Display statistics with the command `show interface vxlan`. Statistics are only displayed once a valid configuration is made on the interface.

### Example

Enabling counters for VXLAN interface 1.

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# vxlan-counters aggregate
```

Disabling counters for VXLAN interface 1.

```
switch(config)# interface vxlan 1
switch(config-vxlan-if)# no vxlan-counters aggregate
```



---

For more information on features that use this command, refer to the VXLAN Guide for your switch model.

---

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context | Authority                                                                                                                                                              |
|---------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9300<br>9300S | config-vxlan-if | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## erase all zeroize

erase [all] zeroize

### Description

Restores the switch to its factory default configuration. You will be prompted before the procedure starts. Once complete, the switch will restart from the primary image with factory default settings.

### Usage

The **erase all** command is always available in the CLI. On running the **erase all** command, the switch is restored to a factory default settings, but retains the enhanced secure mode settings.

The **erase all zeroize** command is not available in the CLI when enhanced secure mode is enabled. This command restore the switch to a factory default settings. On running the **erase all zeroize** command in enhanced secure mode, displays a notification stating that the command is unavailable in enhanced secure mode.



---

Back up all data before running this command as all configuration settings will be lost.

---

### Example

Restoring the switch to factory default configuration, except for the enhance secure mode settings:

```
switch# erase all
This command will erase all data and reset the switch to factory
defaults, with the exception of the secure mode setting. This process
will take several minutes to an hour to complete and the switch will
be unavailable during that time.
Continue (y/n)?
ServiceOS Information:
Version: GT.01.01.0007
Build Date: 2017-12-07 11:48:44 PST
Build ID: ServiceOS:GT.01.01.0007:42c7d15cf7e5:201712071148
SHA: 42c7d15cf7e5af5bf1c7d8764ff673471084c2a4
Preparing for zeroization
Storage zeroization
WARNING: DO NOT POWER OFF UNTIL
ZEROIZATION IS COMPLETE
This should take several minutes
to one hour to complete
Restoring files
```

Restoring the switch to factory default configuration only when enhance secure mode settings is disabled.

```

switch# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
Continue (y/n)? y
The system is going down for zeroization.

...

Preparing for zeroization

Storage zeroization
WARNING: DO NOT POWER OFF UNTIL
ZEROIZATION IS COMPLETE
This should take several minutes
to one hour to complete

Restoring files

...

We'd like to keep you up to date about:
* Software feature updates
* New product announcements
* Special events
Please register your products now at: https://networkingsupport.hpe.com

```



When you log in after zeroization, you get a prompt to create a password for the administrator account. You can set the password as blank (to set the password as blank, hit enter at the prompt) or type 1 to 32 printable ASCII characters, excluding spaces and question marks (?). For more information on password requirements, see *Password requirements* in the *Security Guide*.

```
switch login: admin
Password:

Please configure the 'admin' user account password.
Enter new password: *****
Confirm new password: *****
```



For more information on features that use this command, refer to the Diagnostics and Supportability Guide for your switch model.

## Command History

| Release          | Modification                            |
|------------------|-----------------------------------------|
| 10.11.1010       | Introduced <b>erase all</b> CLI command |
| 10.07 or earlier | --                                      |

## Command Information

| Platforms     | Command context | Authority                                                                          |
|---------------|-----------------|------------------------------------------------------------------------------------|
| All platforms | Manager (#)     | Administrators or local user group members with execution rights for this command. |



### show ztp information

show ztp information

#### Description

Shows information about Zero Touch Provisioning (ZTP) operations performed on the switch.

#### Usage

When a switch configured to use ZTP is booted from a factory default configuration, the switch contacts a DHCP server, which offers options for obtaining files used to provision the switch:

- The IPv4/IPv6 address of TFTP Server or the IPv6 address of HTTP server
- The name of the image file
- The name of the configuration file
- The HPE Aruba Networking Central FDQN or IPv4/IPv6 address
- The HTTP proxy FDQN or IPv4/IPv6 address

The **show ztp information** command shows the options offered by the DHCP server and the status of the ZTP operation.

The status of the ZTP operation is one of the following:

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Success</b>                                                 | The ZTP operation succeeded.<br>One of the following is true: <ul style="list-style-type: none"><li>■ Both the running configuration and the startup configuration were updated.</li><li>■ The IP address of the TFTP/HTTP server was received, but the offer did not include a configuration file or a firmware image file.</li><li>■ Any combination of vendor encapsulated DHCP options are received as configured, along with the firmware image and switch configuration file.</li><li>■ Only vendor encapsulated DHCP options are configured and are received accordingly.</li></ul> |
| <b>Failed - Custom startup configuration detected</b>          | The switch was booted from a configuration that is not the factory default configuration. For example, the administrator password has been set.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Failed - Timed out while waiting to receive ZTP options</b> | Either the switch received the DHCP IPv4 or IPv6 address but no ZTP options were received within 1 minute or ZTP force-provision is triggered and no ZTP options are received within 3 minutes.                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Failed - Detected change in</b>                             | The running configuration was modified by a user while the ZTP operation was in progress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                                                                |                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>running configuration</b>                                   |                                                                                                                                                                                                                                                                                                                            |
| <b>Failed - TFTP server unreachable</b>                        | The TFTP server is not reachable at the specified IP address.                                                                                                                                                                                                                                                              |
| <b>Failed - TFTP server information unavailable</b>            | The image file name or config file name is provided without the TFTP server location to fetch the files from and ZTP enters failed state.                                                                                                                                                                                  |
| <b>Failed - Invalid configuration file received</b>            | Either the file transfer of the configuration file failed, or the configuration file is invalid (an error occurred while attempting to apply the configuration).                                                                                                                                                           |
| <b>Failed - Invalid image file received</b>                    | Either the file transfer of the firmware image file failed, or the firmware image file is invalid (an error occurred while verifying the image).                                                                                                                                                                           |
| <b>Failed - HTTP server unreachable</b>                        | The HTTP server is not reachable at the specified IP address                                                                                                                                                                                                                                                               |
| <b>Failed - Invalid configuration file from USB</b>            | The configuration file is invalid or it is not in the proper format.                                                                                                                                                                                                                                                       |
| <b>Failed - Invalid image file from USB</b>                    | The image file is invalid or it is not in the proper format.                                                                                                                                                                                                                                                               |
| <b>Failed - Error while copying the configuration from USB</b> | ZTP failed to copy the configuration file from the USB device due to a file permissions, file access or system error (for example, if the switch is out of memory), if the user interrupts the ZTP process, or if the file is deleted from the USB device. This message may also display in the event of an unknown error. |
| <b>Failed - Error while copying the image from USB</b>         | ZTP failed to copy the image file from the USB device due to a file permissions, file access or system error (for example, if the switch is out of memory), if the user interrupts the ZTP process, or if the file is deleted from the USB device. This message may also display in the event of an unknown error.         |

In the case of reconnection, connect with a main or alternative location to the COP instance as a user. The current connection is shown in the **Central location** field.

Scenario 1: If the location the device is currently connected on is updated, the system reconnects in order to connect with the new location.

Scenario 2: If the location in which the device is not currently connected on is updated, the DUT does not go through the reconnection process.

## Examples

Showing switch image and config download from an IPv4 TFTP server in progress after receiving ZTP options:



```

switch# show ztp information
TFTP Server : 10.0.0.2
Image File : TL_10_02_0001.swi
Configuration File : ztp.cfg
ZTP Status : In-progress - Image download and verification
HPE ANW Central Location : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Enabled
HTTP Proxy Location : NA

```

Showing switch image download failure from an IPv4 TFTP server because the server was unreachable

```

switch# show ztp information
TFTP Server : 10.0.0.2
Image File : TL_10_02_0001.swi
Configuration File : ztpv6.cfg
ZTP Status : Failed - TFTP server unreachable
HPE ANW Central Location : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Enabled
HTTP Proxy Location : NA

```

Showing a successful switch configuration download from an IPv6 HTTP server

```

switch# show ztp information
HTTP Server : http://[2001::50]
Image File : TL_10_15_0001.swi
Configuration File : config_file
ZTP Status : Success
HPE ANW Central Location : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Enabled
HTTP Proxy Location : NA

```

The switch received image and configuration files from a serial-number specific folder on a USB device, and ZTP was successful.

```

switch# show ztp information
TFTP Server : NA
Image File : usb:/AOSCX/TW88KHD005/GL_10_16_00001.swi
Configuration File : usb:/AOSCX/TW88KHD005/ztp.cfg
Status : Success
HPE ANW Central Location : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Disabled
HTTP Proxy Location : NA

```

The switch received image and configuration files from a generic folder on a USB device, and ZTP was successful.

```
switch# show ztp information
TFTP Server : NA
Image File : usb:/AOSCX/ztp/ML_10_15_1000F.swi
Configuration File : usb:/AOSCX/ztp/config.cfg
Status : Success
HPE ANW Central Location : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Disabled
HTTP Proxy Location : NA
```

The switch received an image file from a vendor-class specific folder on a USB device, and ZTP was successful.

```
switch# show ztp information
TFTP Server : NA
Image File : usb:/AOSCX/8325_JL636A/GL_10_16_1000A.swi
Configuration File : NA
Status : Success
HPE ANW Central Location : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Disabled
HTTP Proxy Location : NA
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification                                                    |
|------------------|-----------------------------------------------------------------|
| 10.16            | The output of this command can show the status of ZTP over USB. |
| 10.07 or earlier | --                                                              |

## Command Information

| Platforms     | Command context             | Authority                                                                                                                                                              |
|---------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only. |

## ztp force provision

```
ztp force-provision
no ztp force-provision
```

### Description

Starts on-demand ZTP via DHCP.

### Usage

DHCP options received are processed independent of the current state of configuration on the switch. Previous ZTP options are cleared, such as the ZTP TFTP server, image file, configuration file, HPE Aruba Networking Central location, and HTTP proxy location, and the switch sends a DHCP request. ZTP using USB is not triggered by this command.

## Examples

In the following example, force-provision is enabled.

```
switch# configure terminal
switch(config)# ztp force-provision
```

In the following example, force-provision status is checked while enabled.

```
switch# show ztp information
TFTP Server : 10.0.0.2
Image File : TL_10_02_0001.swi
Configuration File : ztp.cfg
Status : Success
HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Enabled
HTTP Proxy Location : NA
```

In the following example, force-provision is disabled.

```
switch# configure terminal
switch(config)# no ztp force-provision
```

In the following example, force-provision status is checked while disabled.

```
switch# show ztp information
TFTP Server : 10.0.0.2
Image File : TL_10_02_0001.swi
Configuration File : ztp.cfg
Status : Success
HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision : Disabled
HTTP Proxy Location : NA
```



For more information on features that use this command, refer to the Fundamentals Guide for your switch model.

## Command History

| Release          | Modification |
|------------------|--------------|
| 10.07 or earlier | --           |

## Command Information

| Platforms     | Command context             | Authority                                                                          |
|---------------|-----------------------------|------------------------------------------------------------------------------------|
| All platforms | Operator (>) or Manager (#) | Administrators or local user group members with execution rights for this command. |

### Accessing HPE Aruba Networking Support

|                                             |                                                                                                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HPE Aruba Networking Support Services       | <a href="https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html">https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html</a> |
| AOS-CX Switch Software Documentation Portal | <a href="https://arubanetworking.hpe.com/techdocs/AOS-CX/help_portal/Content/home.htm">https://arubanetworking.hpe.com/techdocs/AOS-CX/help_portal/Content/home.htm</a>       |
| HPE Aruba Networking Support Portal         | <a href="https://networkingsupport.hpe.com/home">https://networkingsupport.hpe.com/home</a>                                                                                   |
| North America telephone                     | 1-800-943-4526 (US & Canada Toll-Free Number)<br>+1-650-750-0350 (Backup—Toll Number)                                                                                         |
| International telephone                     | <a href="https://www.hpe.com/psnow/doc/a50011948enw">https://www.hpe.com/psnow/doc/a50011948enw</a>                                                                           |

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

#### Other useful sites

Other websites that can be used to find information:

|                                                      |                                                                                                                                                                                                                       |
|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HPE Aruba Networking Developer Hub                   | <a href="https://developer.arubanetworks.com/hpe-aruba-networking-aoscx/docs/about">https://developer.arubanetworks.com/hpe-aruba-networking-aoscx/docs/about</a>                                                     |
| Airheads social forums and Knowledge Base            | <a href="https://community.arubanetworks.com/">https://community.arubanetworks.com/</a>                                                                                                                               |
| AOS-CX Software Technical Update channel on YouTube. | Videos on new features introduced in this release:<br><a href="https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS">https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS</a> |

|                                                                     |                                                                                                                                                                                             |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HPE Aruba Networking Hardware Documentation and Translations Portal | <a href="https://arubanetworking.hpe.com/techdocs/hardware/DocumentationPortal/Content/home.htm">https://arubanetworking.hpe.com/techdocs/hardware/DocumentationPortal/Content/home.htm</a> |
| HPE Aruba Networking software                                       | <a href="https://networkingsupport.hpe.com/downloads">https://networkingsupport.hpe.com/downloads</a>                                                                                       |
| Software licensing and Feature Packs                                | <a href="https://licensemanagement.hpe.com/">https://licensemanagement.hpe.com/</a>                                                                                                         |
| End-of-Life information                                             | <a href="https://networkingsupport.hpe.com/end-of-life">https://networkingsupport.hpe.com/end-of-life</a>                                                                                   |

## Accessing Updates

You can access updates from the HPE Aruba Networking Support Portal at <https://networkingsupport.hpe.com>.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

<https://networkingsupport.hpe.com/notifications/subscriptions> (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Portal account.

## Warranty Information

To view warranty information for your product, go to <https://www.arubanetworks.com/support-services/product-warranties/>.

## Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at <https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

### Additional regulatory information

HPE Aruba Networking is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see <https://www.arubanetworks.com/company/about-us/environmental-citizenship/>.

## Documentation Feedback

HPE Aruba Networking is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback



([docsfeedback-switching@hpe.com](mailto:docsfeedback-switching@hpe.com)). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.