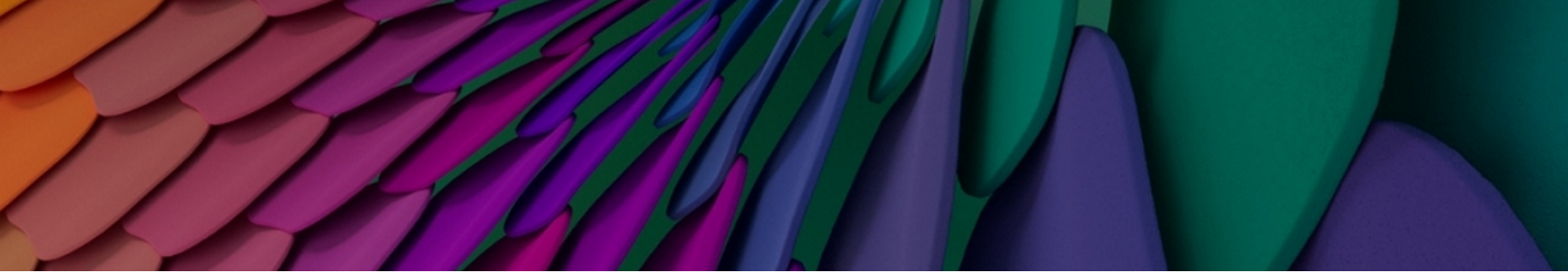

AOS-CX 10.14 Command-Line Interface Guide

6000, 6100 Switch Series

aruba
a Hewlett Packard Enterprise company

Published: April 2024

Edition: 1

Copyright Information

© Copyright 2024 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.

Contents 3

About this document 28
- Applicable products 28
- What's new in this release 28
- Latest version available online 29
- Command syntax notation conventions 29
- About the examples 29
- Identifying switch ports and interfaces 30

Introduction to the AOS-CX CLI 31
- CLI access 31
- Getting CLI help 31
- Authority levels 32
- Command contexts 33
  - Operator context (>) 33
  - Navigating to the operator context (>) 33
  - Auditor context 33
  - Manager context (#) 34
  - Navigating to the manager context (#) 34
  - Global configuration context (config) 34
  - Navigating to the config context 35
  - Other configuration command contexts 35
  - Support for range contexts 36
  - Rules for range contexts 38
- Command history 38
- Command completion 39
- Pipe (|) support in show commands 39
- Command syntax notation conventions 40

Service OS CLI commands 41
- boot 41
- cat 42
- cd path 42
- config-clear 43
- cp 44
- du 45
- erase zeroize 46
- exit 47
- format 48
- identify 49
- ls 50
- md5sum 51
- mkdir 52
- mount 53
- mv 54

password (svos) 55
pwd 55
reboot 56
rm 57
rmdir 57
secure-mode 58
sh 60
system serviceos password-prompt 60
umount 61
update 62
version 63

ACL commands 65
ACL application 65
access-list copy 65
access-list ip 69
access-list ipv6 79
access-list log-timer 87
access-list mac 90
access-list resequence 95
access-list reset 98
access-list secure-update 101
apply access-list control-plane 103
apply access-list (to interface or LAG) 104
apply access-list (to L3 VNI) 106
apply access-list (to VLAN) 106
clear access-list hitcounts 108
clear access-list hitcounts control-plane 109
show access-list 110
show access-list control-plane 114
show access-list hitcounts 116
show access-list hitcounts control-plane 119
show access-list secure-update 120
location-override-alternative 121
show capacities 122
show capacities-status 125

ACL and Policy hardware resource commands 128
show resources 128

ARP commands 133
arp inspection 133
arp inspection trust 133
arp ip 134
arp process-grat-arp 135
clear arp 136
debug arp-security 137
ip proxy-arp 139
ipv6 neighbor mac 140
show arp 141
show arp inspection interface 142
show arp inspection statistics 143
show arp inspection vlan 144
show arp state 145
show arp summary 146
show arp timeout 147

show arp vrf 148
show ipv6 neighbors 149
show ipv6 neighbors state 150
show tech arp-security 152

Banner commands 154
banner 154
show banner 155

Boot commands 157
boot set-default 157
boot system 157
show boot-history 159

Cable diagnostic commands 162
diag cable-diagnostic 162

Captive portal (RADIUS) commands 165
aaa authentication port-access captive-portal-profile 165
show port-access captive-portal-profile 166
url 167
url-hash-key 168

CDP commands 171
cdp 171
clear cdp counters 172
clear cdp neighbor-info 172
show cdp 173
show cdp neighbor-info 174
show cdp traffic 175
show cdp voice-vlan mode 176

Checkpoint commands 178
checkpoint auto 178
checkpoint auto confirm 179
checkpoint diff 180
checkpoint post-configuration 182
checkpoint post-configuration timeout 183
checkpoint rename 184
checkpoint rollback 184
copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL> 185
copy checkpoint <CHECKPOINT-NAME> {running-config | startup-config} 187
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL> 187
copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME> 188
copy <REMOTE-URL> {running-config | startup-config} 189
copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>} 191
copy {running-config | startup-config} <REMOTE-URL> 192
copy {running-config | startup-config} <STORAGE-URL> 194
copy startup-config running-config 195
copy <STORAGE-URL> running-config 195
erase 197
show checkpoint <CHECKPOINT-NAME> 198
show checkpoint <CHECKPOINT-NAME> hash 200
show checkpoint post-configuration 201
show checkpoint 202

show checkpoint date ... 203
show running-config hash ... 204
show startup-config hash ... 205
write memory ... 206

Classifier policy commands ... 207

Classifier policy application ... 207
apply policy (config-if, config-lag-if, config-vlan) ... 207
apply policy ... 210
class copy ... 211
class ip ... 212
class ipv6 ... 219
class resequence ... 225
class reset ... 227
clear policy hitcounts ... 228
policy ... 228
policy copy ... 233
policy resequence ... 234
policy reset ... 235
show class ... 236
show policy ... 237

Client Insight Commands ... 242

client-insight enable ... 242
client-insight on-boarding event logs ... 242
diag-dump client-insight basic ... 243
show capacities client-insight-client-limit ... 245
show capacities-status client-insight-client-limit ... 246
show events -c client-insight ... 247
show tech client-insight ... 249

CLI session commands ... 254

alias ... 254
auto-confirm ... 255
configure terminal ... 256
disable ... 257
do ... 257
enable (manager context) ... 258
end ... 259
exit ... 259
list ... 260
page ... 261
Pipe (|) command ... 262
repeat ... 263
session-timeout ... 263
show session-timeout ... 264
show alias ... 265
show history ... 265

CLI user session management commands ... 268

cli-session ... 268

Clock commands ... 271

clock date ... 271
clock datetime ... 271
clock time ... 272

clock timezone ... 273
show clock ... 273

CoPP commands ... 275

Classes of traffic ... 275
apply copp-policy ... 276
class ... 277
clear copp-policy statistics ... 278
copp-policy ... 278
default-class ... 280
reset copp-policy ... 280
show copp-policy ... 282
show copp-policy factory-default ... 283
show copp-policy statistics ... 285
show tech copp ... 286

Debug logging commands ... 288

clear debug buffer ... 288
debug {all | <MODULE-NAME>} ... 289
debug db ... 290
debug destination ... 292
show debug ... 294
show debug buffer ... 295
show debug destination ... 296

Device profile commands ... 297

aaa authentication port-access allow-cdp-auth ... 297
aaa authentication port-access allow-cdp-bpdu ... 298
aaa authentication port-access allow-cdp-proxy-logoff ... 299
aaa authentication port-access allow-lldp-bpdu ... 300
associate cdp-group ... 302
associate lldp-group ... 303
associate mac-group ... 304
associate role ... 305
disable ... 305
enable ... 306
ignore (for CDP groups) ... 307
ignore (for LLDP groups) ... 308
ignore (for MAC groups) ... 309
mac-group ... 315
match (for CDP groups) ... 316
match (for LLDP groups) ... 317
match (for MAC groups) ... 319
port-access cdp-group ... 323
port-access device-profile ... 324
port-access device-profile mode block-until-profile-applied ... 325
port-access lldp-group ... 326
show port-access device-profile ... 327

DHCP client commands ... 330

ip dhcp ... 330
ip dhcp option ... 331
show ip dhcp ... 332

DHCPv4 relay commands ... 333

dhcp-relay l2vpn-clients ... 333

show dhcp-relay 334
show dhcp-relay bootp-gateway 334
show ip helper-address 335

DHCP relay (IPv6) commands 337
show dhcpv6-relay 337
show ipv6 helper-address 337

DHCP snooping commands 339
clear dhcp-snooping binding 339
clear dhcp-snooping statistics 340
dhcp-snooping 341
dhcp-snooping (in config-vlan context) 341
dhcp-snooping allow-overwrite-binding 342
dhcp-snooping authorized-server 343
dhcp-snooping event-log client 344
dhcp-snooping external-storage 345
dhcp-snooping flash-storage 347
dhcp-snooping max-bindings 348
dhcp-snooping option 82 349
dhcp-snooping static-attributes 350
dhcp-snooping trust 351
dhcp-snooping verify mac 352
show dhcp-snooping 353
show dhcp-snooping binding 355
show dhcp-snooping statistics 356

DHCPv6 snooping commands 358
clear dhcpv6-snooping binding 358
clear dhcpv6-snooping statistics 359
dhcpv6-snooping 359
dhcpv6-snooping (in config-vlan context) 360
dhcpv6-snooping authorized-server 361
dhcpv6-snooping event-log client 362
dhcpv6-snooping external-storage 363
dhcpv6-snooping flash-storage 365
dhcpv6-snooping max-bindings 366
dhcpv6-snooping trust 367
show dhcpv6-snooping 368
show dhcpv6-snooping binding 369
show dhcpv6-snooping statistics 370

DHCP options commands 372
http-proxy 372

DNS client commands 374
ip dns domain-list 374
ip dns domain-name 375
ip dns host 376
ip dns server address 377
show ip dns 378
redistribute local-mac 379

Fault monitor commands 380
(Fault enabling/disabling) 380

action 381
apply fault-monitor profile 384
fault-monitor profile 385
show fault-monitor profile 386
show interface fault-monitor profile 388
show interface fault-monitor status 389
show running-config 389
threshold 391

Firmware management commands 394
copy {primary | secondary} <REMOTE-URL> 394
copy {primary | secondary} <FIRMWARE-FILENAME> 395
copy primary secondary 396
copy <REMOTE-URL> 396
copy secondary primary 398
copy <STORAGE-URL> 399
copy hot-patch 400
hot-patch 402
show hot-patch 403

HTTPS server commands 405
https-server max-user-sessions 405
https-server rest access-mode 405
https-server rest firmware-site-distribution 407
https-server session close all 407
https-server session-timeout 408
https-server vrf 409
show https-server 410
show https-server authentication 411

ICMP commands 413
ip icmp redirect 413
ip icmp throttle 413
ip icmp unreachable 414

IGMP commands 416
ip igmp 416
ip igmp apply access-list 417
ip igmp last-member-query-interval 418
ip igmp querier 419
ip igmp querier interval 420
ip igmp querier-wait-time 421
ip igmp querier query-max-response-time 422
ip igmp robustness 423
ip igmp router-alert-check 424
ip igmp static-group 425
ip igmp version 426
ip igmp version strict 426
no ip igmp 427
show ip igmp 428
show ip igmp counters 429
show ip igmp group 430
show ip igmp groups 433
show ip igmp interface 435
show ip igmp interface counters 436
show ip igmp interface group 437

show ip igmp interface groups 439
show ip igmp interface statistics 440
show ip igmp static-groups 441
show ip igmp statistics 442

IGMP snooping commands 444

ip igmp snooping apply access list 444
ip igmp snooping (config mode) 445
ip igmp snooping filter unknown mcast 446
ip igmp snooping (interface mode) 447
ip igmp snooping preprogram-starg-flow 449
ip igmp snooping static group 451
ip igmp snooping (vlan mode) 452
show ip igmp snooping 453

In-System Programming commands 457

clear update-log 457
show needed-updates 457

Interface commands 459

allow-unsupported-transceiver 459
default interface 460
description 461
energy-efficient-ethernet 462
flow-control 463
interface 464
interface vlan 465
ip address 466
ip mtu 467
ipv6 address 467
mtu 469
persona 470
rate-interval 472
show allow-unsupported-transceiver 473
show interface 474
show interface dom 479
show interface energy-efficient ethernet 480
show interface flow-control 481
show interface statistics 486
show interface transceiver 489
show interface utilization 492
show ip interface 493
show ip source-interface 494
show ipv6 interface 495
show ipv6 source-interface 497
shutdown 498
speed 498

IP Client Tracker commands 502

client track ip 502
client track ip { enable | disable | auto } 503
client track ip client-limit 504
client track ip update-interval 504
client track ip update-method probe 505
show capacities 506
show client ip { count | port | vlan } 507

IPv4 source lockdown commands 508
ipv4 source-binding 508
ipv4 source-lockdown 509
ipv4 source-lockdown hardware retry 510
show ipv4 source-binding 511
show ipv4 source-lockdown 511
IPv6 RA commands 516
ipv6 address <global-unicast-address> 516
ipv6 address autoconfig 517
ipv6 address link-local 518
ipv6 nd cache-limit 518
ipv6 nd dad attempts 519
ipv6 nd hop-limit 520
ipv6 nd mtu 521
ipv6 nd ns-interval 521
ipv6 nd prefix 522
ipv6 nd ra dns search-list 524
ipv6 nd ra dns server 525
ipv6 nd ra lifetime 526
ipv6 nd ra managed-config-flag 527
ipv6 nd ra max-interval 528
ipv6 nd ra min-interval 529
ipv6 nd ra other-config-flag 529
ipv6 nd ra reachable-time 530
ipv6 nd ra retrans-timer 531
ipv6 nd route 532
ipv6 nd router-preference 533
ipv6 nd suppress-ra 534
show ipv6 nd global traffic 534
show ipv6 nd interface 535
show ipv6 nd interface prefix 540
show ipv6 nd interface route 541
show ipv6 nd ra dns search-list 542
show ipv6 nd ra dns server 543
IPv6 source lockdown commands 544
ipv6 source-binding 544
ipv6 source-lockdown 545
ipv6 source-lockdown hardware retry 546
show ipv6 source-binding 547
show ipv6 source-lockdown 547
IRDP commands 552
diag-dump irdp basic 552
ip irdp 553
ip irdp holdtime 554
ip irdp maxadvertinterval 555
ip irdp minadvertinterval 556
ip irdp preference 557
show ip irdp 558
Job Scheduler commands 560
job 560
schedule 562

show job 565
show capacities (job, schedule) 568
show running-config (job, schedule) 568
show schedule 570

Key chain commands 573
accept-lifetime 573
key 574
keychain 575
key-string 576
name 577
recv-id 578
send-lifetime 579
send-id 580
show capacities keychain 581
show keychain 582
show running-config keychain 583

L1-100Mbps downshift commands 585
downshift enable 585
show interface 586
show interface downshift-enable 591
show running-config interface 592

LACP and LAG commands 594
description 594
interface lag 595
lacp fallback-static 596
lacp hash 597
lacp mode 597
lacp port-id 598
lacp port-priority 599
lacp rate 600
lacp system-priority 601
lag 602
show interface 603
show lacp aggregates 604
show lacp configuration 605
show lacp interfaces 606
show lag 610
show running-config interface lag 611
shutdown 612
vlan trunk native 613

LLDP commands 615
clear lldp neighbors 615
clear lldp statistics 615
lldp 616
lldp dot3 617
lldp dot3 eee 618
lldp dot3 mfs 618
lldp holdtime-multiplier 619
lldp management-address vlan 620
lldp management-ip-address 621
lldp management-ipv6-address 622
lldp med 623

lldp med location 624
lldp receive 627
lldp reinit 627
lldp select-tlv 628
lldp timer 629
lldp transmit 631
lldp txdelay 632
lldp trap enable 632
show lldp configuration 635
show lldp local-device 636
show lldp neighbor-info 638
show lldp neighbor-info detail 640
show lldp statistics 643
show lldp tlv 644

Local AAA commands 646
aaa accounting all-mgmt 646
aaa authentication console-login-attempts 648
aaa authentication limit-login-attempts 649
aaa authentication login 650
aaa authentication minimum-password-length 651
aaa authorization commands (local) 652
show aaa accounting 654
show aaa authentication 655
show aaa authorization 656
show authentication locked-out-users 657
show ssh authentication-method 658
show user 658
ssh password-authentication 660
ssh public-key-authentication 660
user authorized-key 661

Log rotation commands 663
logging threshold 663
logrotate maxsize 664
logrotate period 665
logrotate target 666
show logrotate 668

Loop protect commands 669
loop-protect 669
loop-protect action 670
loop-protect re-enable-timer 671
loop-protect transmit-interval 672
loop-protect trap loop-detected 672
loop-protect vlan 673
show loop-protect 674

Loopback commands 678
interface loopback 678
ip address 678
ipv6 address 679
show interface loopback 680

MAC address table commands 682
clear mac-address 682

clear mac address mac move 684
clear mac-address-table 685
mac-address-table age-time 686
show mac-address-table 686
show mac-address-table address 687
show mac-address-table count 688
show mac-address-table dynamic 689
show mac-address-table interface 690
show mac-address-table lockout 691
show mac address table mac move 692
show mac-address-table mac-move 693
show mac-address-table port 695
show mac-address-table static 695
show mac-address-table vlan 696
show mac address table mac move 697
static-mac 698

Mirroring commands 700
clear mirror 700
comment 700
destination interface 702
destination tunnel 703
diagnostic 704
disable 705
enable 706
mirror endpoint 707
mirror session 708
show mirror 709
show mirror endpoint 711
source interface 712

MLD snooping global configuration commands 715
ipv6 mld snooping 715

MLD snooping VLAN configuration commands 716
ipv6 mld snooping 716
ipv6 mld snooping fastlearn 717
ipv6 mld snooping fastleave vlan 717
ipv6 mld snooping filter-unknown-mcast 718
ipv6 mld snooping forced fastleave vlan 719
ipv6 mld snooping apply access-list 720
ipv6 mld snooping auto vlan 722
ipv6 mld snooping blocked vlan 722
ipv6 mld snooping forward vlan 723
ipv6 mld snooping preprogram-starg-flow 724
ipv6 mld snooping static-group 726
ipv6 mld snooping version 726

MLD snooping show commands 728
show ipv6 mld snooping 728

MLD configuration commands for interface VLAN 732
ipv6 mld 732
ipv6 mld apply access-list 732
no ipv6 mld 734
ipv6 mld querier 734

ipv6 mld querier interval 735
ipv6 mld querier-wait-time 736
ipv6 mld last-member-query-interval 736
ipv6 mld querier query-max-response-time 737
ipv6 mld robustness 738
ipv6 mld static-group 739
ipv6 mld version 739
ipv6 mld version strict 740

MLD show commands for interface VLAN 742
show ipv6 mld 742

MLD configuration commands for interface 746
ipv6 mld 746
ipv6 mld apply access-list 746
no ipv6 mld 748
ipv6 mld querier 748
ipv6 mld querier interval 749
ipv6 mld last-member-query-interval 750
ipv6 mld querier query-max-response-time 750
ipv6 mld robustness 751
ipv6 mld static-group 752
ipv6 mld version 753
ipv6 mld version strict 753

MSTP commands 755
clear spanning-tree statistics 755
show spanning-tree 755
show spanning-tree detail 757
show spanning-tree inconsistent-ports 758
show spanning-tree mst 759
show spanning-tree mst-config 762
show spanning-tree mst detail 762
show spanning-tree mst <INSTANCE-ID> 766
show spanning-tree mst <INSTANCE-ID> detail 767
show spanning-tree mst interface 768
show spanning-tree summary port 769
show spanning-tree summary root 770
spanning-tree 771
spanning-tree bpdu-filter 772
spanning-tree bpdu-guard 773
spanning-tree bpdu-guard timeout 774
spanning-tree config-name 775
spanning-tree config-revision 776
spanning-tree cost 777
spanning-tree forward-delay 778
spanning-tree hello-time 779
spanning-tree instance cost 780
spanning-tree instance port-priority 781
spanning-tree instance priority 782
spanning-tree instance vlan 783
spanning-tree link-type 784
spanning-tree loop-guard 784
spanning-tree max-age 785
spanning-tree max-hops 786
spanning-tree mode 787

spanning-tree port-priority 789
spanning-tree port-type 790
spanning-tree priority 791
spanning-tree root-guard 792
spanning-tree rpvst-filter 793
spanning-tree rpvst-guard 794
spanning-tree tcn-guard 795
spanning-tree transmit-hold-count 796
spanning-tree trap 796

MVRP commands 799
clear mvrp statistics 799
mvrp 799
mvrp registration 800
mvrp timer 801
show mvrp config 802
show mvrp state 803
show mvrp statistics 804

NTP commands 806
ntp authentication 806
ntp authentication-key 806
ntp disable 808
ntp enable 808
ntp server 809
ntp trusted-key 811
ntp vrf 812
show ntp associations 813
show ntp authentication-keys 814
show ntp servers 815
show ntp statistics 815
show ntp status 816

Ping commands 818
ping 818
ping6 823

PKI commands 827
crypto pki application 827
crypto pki certificate 828
crypto pki ta-profile 829
enroll self-signed 830
enroll terminal 831
import (CA-signed leaf certificate) 832
import (self-signed leaf certificate) 834
key-type 836
ocsp disable-nonce 837
ocsp enforcement-level 838
ocsp url 839
ocsp vrf 840
revocation-check ocsp 841
show crypto pki application 842
show crypto pki certificate 843
show crypto pki ta-profile 845
ta-certificate 847
subject 848

PKI EST commands 850

arbitrary-label 850
arbitrary-label-enrollment 851
arbitrary-label-reenrollment 852
crypto pki est-profile 853
enroll est-profile 854
reenrollment-lead-time 855
retry-count 856
retry-interval 857
show crypto pki est-profile 858
url 859
username 860
vrf 862

PoE commands 864

lldp dot3 poe 864
lldp med poe 865
power-over-ethernet 865
power-over-ethernet allocate-by 866
power-over-ethernet assigned-class 868
power-over-ethernet pre-std-detect 869
power-over-ethernet priority 869
power-over-ethernet threshold 870
power-over-ethernet trap 871
show lldp local 872
show lldp neighbor 873
show power-over-ethernet 874

Port access 802.1X authentication commands 877

aaa authentication port-access dot1x authenticator 877
aaa authentication port-access dot1x authenticator auth-method 878
aaa authentication port-access dot1x authenticator cached-reauth 879
aaa authentication port-access dot1x authenticator cached-reauth-period 879
aaa authentication port-access dot1x authenticator discovery-period 880
aaa authentication port-access dot1x authenticator eap-tls-fragment 881
aaa authentication port-access dot1x authenticator eapol-timeout 882
aaa authentication port-access dot1x authenticator initial-auth-response-timeout 883
aaa authentication port-access dot1x authenticator max-eapol-requests 884
aaa authentication port-access dot1x authenticator max-retries 885
aaa authentication port-access dot1x authenticator quiet-period 886
aaa authentication port-access dot1x authenticator radius server-group 887
aaa authentication port-access dot1x authenticator reauth 888
aaa authentication port-access dot1x authenticator reauth-period 889
clear dot1x authenticator statistics interface 890
show aaa authentication port-access dot1x authenticator interface client-status 891
show aaa authentication port-access dot1x authenticator interface port-statistics 892

Port access 802.1X supplicant commands 895

aaa authentication port-access dot1x supplicant(global) 895
aaa authentication port-access dot1x supplicant(port) 895
associate policy 896
canned-eap-success 898
clear dot1x supplicant statistics 898
discovery-timeout 900
eap-identity 901

eapol-force-multicast ... 903
eapol-method ... 904
eapol-protocol-version ... 905
eapol-timeout ... 907
enable ... 908
enable ... 909
fail-mode ... 909
held-period ... 910
max-retries ... 912
policy (supplicant) ... 913
port-access dot1x supplicant restart ... 914
show aaa authentication port-access dot1x supplicant policy ... 915
show aaa authentication port-access dot1x supplicant statistics ... 917
show aaa authentication port-access dot1x supplicant status ... 919
start-mode ... 922

Port access cached-critical role commands ... 924

aaa authentication port-access cached-critical-role (global) ... 924
aaa authentication port-access cached-critical-role (per interface) ... 926
port-access clear cached-client ... 927
show port-access cached-clients ... 928
show port-access cached-critical-role info ... 929

Port access general commands ... 931

aaa authentication port-access allow-lldp-auth ... 931
aaa authentication port-access auth-mode ... 933
aaa authentication port-access auth-precedence ... 934
aaa authentication port-access auth-priority ... 935
aaa authentication port-access auth-role ... 937
aaa authentication port-access client-auto-log-off final-authentication-failure ... 938
aaa authentication port-access client-limit ... 939
aaa authentication port-access client-limit multi-domain ... 940
aaa authentication port-access radius-override ... 940
port-access allow-flood-traffic ... 942
port-access client-move ... 943
port-access event-log client ... 944
port-access fallback-role ... 945
port-access log-off client ... 946
port-access onboarding-method precedence ... 947
port-access onboarding-method concurrent ... 948
port-access reauthenticate interface ... 949
show aaa authentication port-access interface client-status ... 950
show port-access clients ... 952
show port-access clients detail ... 955
show port-access clients onboarding-method ... 958
show port-access interface ... 959

Port access MAC authentication commands ... 961

aaa authentication port-access mac-auth ... 961
aaa authentication port-access mac-auth addr-format ... 962
aaa authentication port-access mac-auth auth-method ... 962
aaa authentication port-access mac-auth cached-reauth ... 963
aaa authentication port-access mac-auth cached-reauth-period ... 964
aaa authentication port-access mac-auth password ... 965
aaa authentication port-access mac-auth quiet-period ... 966
aaa authentication port-access mac-auth radius server-group ... 967

aaa authentication port-access mac-auth reauth 968
aaa authentication port-access mac-auth reauth-period 969
clear mac-auth statistics 970
show aaa authentication port-access mac-auth interface client-status 970
show aaa authentication port-access mac-auth interface port-statistics 972

Port access policy commands 974
port-access policy 974
port-access policy copy 978
port-access policy resequence 979
port-access policy reset 979
clear port-access policy hitcounts 981
show port-access policy 983
show port-access policy hitcounts 985

Port access role commands 988
associate policy 988
auth-mode 989
cached-reauth-period 990
client-inactivity timeout 991
description 992
device-traffic-class 992
mtu 993
poe-allocate-by 994
poe-priority 995
port-access role 996
reauth-period 997
session timeout 998
show aaa authentication port-access interface client-status 998
show port-access role 1000
stp-admin-edge-port 1001
trust-mode 1002
vlan 1003

Port access security violation commands 1006
port-access security violation action 1006
port-access security violation action shutdown auto-recovery 1007
port-access security violation action shutdown recovery-timer 1008
show interface 1009
show port-access aaa violation interface 1009
show port-access port-security violation client-limit-exceeded interface 1011

Port access VLAN group commands 1013
associate-vlan 1013
port-access vlan-group 1014
show running-config port-access vlan-group 1015

Port filtering commands 1016
portfilter 1016
show portfilter 1017

Port security commands 1019
port-access port-security 1019
port-access port-security client-limit 1020
port-access port-security mac-address 1021

show port-access port-security interface client-status 1021
show port-access port-security interface port-statistics 1023
show port-access security violation sticky-mac-client-move interface 1024
sticky-learn enable 1025

Private VLAN commands 1026

diag-dump private-vlan basic 1026
private-vlan 1026
private-vlan port-type 1028
show capacities private-vlan 1029
show capacities-status private-vlan 1030
show private-vlan 1030
show private-vlan association 1032
show private-vlan inconsistency 1033
show private-vlan port-type 1035
show running-configuration private-vlan 1035
show tech private-vlan 1036

QoS commands 1039

apply qos 1039
map queue 1041
min-bandwidth 1042
name queue 1044
qos cos 1044
qos dscp 1045
qos dscp-map 1047
qos queue-profile 1048
qos schedule-profile 1049
qos trust 1051
rate-limit 1053
show interface queues 1056
show interface qos 1058
show qos dscp-map 1058
show qos queue-profile 1060
show qos schedule-profile 1061
show qos trust 1062
strict queue 1063

Configurable RADIUS attribute commands 1066

aaa radius-attribute group 1066
nas-id request-type 1067
nas-id value 1068
nas-ip-addr request-type authentication 1069
nas-ip-addr service-type user-management 1070
tunnel-private-group-id request-type 1071
tunnel-private-group-id value 1072

RADIUS dynamic authorization commands 1074

radius dyn-authorization enable 1074
radius dyn-authorization client 1074
radius dyn-authorization client tls (RadSec) 1076
radius dyn-authorization port 1078
show radius dyn-authorization 1079
show radius dyn-authorization client 1081
show radius dyn-authorization client tls (RadSec) 1082

Remote AAA (TACACS+, RADIUS) commands 1085

aaa accounting allow-fail-through 1085
aaa accounting all-mgmt 1085
aaa authentication allow-fail-through 1088
aaa authentication login 1089
aaa authorization allow-fail-through 1091
aaa authorization commands 1093
aaa group server 1096
radius-server auth-type 1097
radius-server host 1098
radius-server host secure ipsec 1101
radius-server host tls port-access 1106
radius-server host tls tracking-method 1108
radius-server key 1109
radius-server retries 1110
radius-server status-server interval 1111
radius-server timeout 1112
radius-server tracking 1113
server 1115
show aaa accounting 1117
show aaa authentication 1119
show aaa authorization 1121
show aaa server-groups 1123
show accounting log 1125
show radius-server 1128
show radius-server secure ipsec 1133
show tacacs-server 1134
show tacacs-server statistics 1137
show tech aaa 1137
tacacs-server auth-type 1143
tacacs-server host 1144
tacacs-server key 1146
tacacs-server timeout 1148
tacacs-server tracking 1149

Remote syslog commands 1151

clear accounting-logs 1151
logging 1152
logging accounting-format-native 1154
logging filter 1155
logging facility 1159
logging persistent-storage 1159

RPVST+ commands 1162

clear spanning-tree statistics 1162
show capacities rpvst 1162
show capacities-status rpvst 1163
show spanning-tree 1164
show spanning-tree detail 1165
show spanning-tree inconsistent-ports 1167
show spanning-tree summary port 1168
show spanning-tree summary root 1169
show spanning-tree vlan 1170
show spanning-tree vlan detail 1171
spanning-tree bpdu-guard timeout 1173
spanning-tree extend-system-id 1173

spanning-tree ignore-pvid-inconsistency ... 1174
spanning-tree link-type ... 1176
spanning-tree mode ... 1176
spanning-tree pathcost-type ... 1178
spanning-tree rpvst-mstp interconnect vlan ... 1179
spanning-tree tcn-guard ... 1180
spanning-tree vlan ... 1181
spanning-tree vlan cost ... 1182
spanning-tree vlan port-priority ... 1183
spanning-tree trap ... 1184

Runtime diagnostic commands ... 1187
diagnostic monitor ... 1187
diag on-demand ... 1188
show diagnostic ... 1189
show diagnostic events ... 1191

Selftest commands ... 1193
fastboot ... 1193
show selftest ... 1194

sFlow agent commands ... 1197
clear sflow statistics ... 1197
sflow ... 1197
sflow agent-ip ... 1199
sflow collector ... 1200
sflow disable ... 1201
sflow header-size ... 1201
sflow max-datagram-size ... 1202
sflow polling ... 1203
sflow sampling ... 1204
show sflow ... 1205

Smartlink commands ... 1207
Configuration commands ... 1207
smartlink group ... 1207
smartlink recv-control-vlan ... 1208
Group context commands ... 1208
description ... 1208
diag-dump smartlink basic ... 1209
primary-port ... 1210
smartlink group secondary-port ... 1211
control-vlan ... 1212
protected-vlans ... 1213
preemption ... 1214
preemption-delay ... 1214
Display commands ... 1215
show smartlink group ... 1215
show smartlink group all ... 1216
show smartlink group detail ... 1217
show smartlink flush-statistics ... 1218
clear smartlink group statistics ... 1219
clear smartlink flush-statistics ... 1219
show running-config ... 1220
Supportability commands ... 1221
show capacities smartlink ... 1221

SNMP commands 1223

event-trap-enable 1223
lldp trap enable 1223
mac-notify traps 1226
rmon alarm 1228
rmon alarm {enable | disable} {index | all} 1230
show configuration-changes trap 1230
show mac-notify 1231
show mac-notify port 1232
show rmon alarm 1233
show snmp agent-port 1234
show snmp community 1235
show snmp system 1236
show snmp trap 1237
show snmp views 1238
show snmp vrf 1239
show snmpv3 context 1240
show snmpv3 engine-id 1240
show snmpv3 security-level 1241
show snmpv3 users 1242
snmp-server agent-port 1242
snmp-server community 1243
snmp-server community view 1246
snmp-server historical-counters-monitor 1247
snmp-server response-source 1247
snmp-server host 1249
snmp-server system-contact 1252
snmp-server system-description 1253
snmp-server system-location 1254
snmp-server trap aaa-server-reachability-status 1255
snmp-server trap configuration-changes 1256
snmp-server trap mac-notify 1256
snmp-server trap port-security 1257
snmp-server trap snmp 1258
snmp-server trap-source interface vrf 1259
snmp-server trap vsx 1260
snmp-server view 1261
snmp-server vrf 1262
snmpv3 context 1263
snmpv3 engine-id 1264
snmpv3 security-level 1265
snmpv3 user 1266
snmpv3 user view 1270

Source-interface selection commands 1272

ip source-interface 1272
ipv6 source-interface 1274
ipv6 source-interface dns 1276
show ip source-interface 1279
show ipv6 source-interface 1280
show running-config 1283
SSH client commands 1285
ssh (client login) 1285

SSH client commands 1287

ssh (client login) 1287

SSH server commands 1289
show ssh host-key 1289
show ssh server 1290
show ssh server sessions 1291
ssh ciphers 1292
ssh host-key 1293
ssh host-key-algorithms 1295
ssh key-exchange-algorithms 1296
ssh known-host remove 1297
ssh macs 1298
ssh maximum-auth-attempts 1299
ssh public-key-algorithms 1300
ssh server allow-list 1301
ssh server port 1303
ssh server vrf 1304

Static routing commands 1306
ip route 1306
ip route distance 1307
ip route tag 1308
ipv6 route 1309
ipv6 route distance 1310
ipv6 route tag 1311
show ip rib 1312
show ipv6 rib 1315

Supportability copy commands 1319
copy checkpoint 1319
copy command-output 1320
copy diag-dump feature <FEATURE> 1321
copy diag-dump local-file 1322
copy <IMAGE> 1323
copy running-config 1325
copy show-tech feature 1326
copy show-tech local-file 1327
copy startup-config 1328
copy support-files 1329
copy support-files local-file 1331
copy support-log 1332

Switch system and hardware commands 1335
clear events 1335
console baud-rate 1336
domain-name 1337
front-panel-security factory-reset 1338
front-panel-security factory-reset 1339
hostname 1340
show boot-history 1341
show capacities 1343
show capacities-status 1350
show console 1352
show core-dump 1352
show deprecated commands 1354
show domain-name 1355
show environment fan 1356

show environment led 1357
show environment power-supply 1358
show environment temperature 1359
show events 1361
show front-panel-security status 1363
show hostname 1365
show images 1365
show module 1366
show running-config 1368
show running-config current-context 1373
show startup-config 1374
show system 1375
show system resource-utilization 1376
show tech 1378
show usb 1380
show usb file-system 1381
show version 1382
system resource-utilization poll-interval 1383
top cpu 1384
top memory 1385
usb 1385
usb mount | unmount 1386

Telnet commands 1388
show telnet server 1388
show telnet server sessions 1388
telnet server 1389

Terminal monitor commands 1391
logging console {notify | severity | filter} 1391
show terminal-monitor 1392
terminal-monitor {notify | severity | filter} 1393

Traceroute commands 1395
traceroute 1395
traceroute6 1397

Two-factor authentication commands 1400
aaa authorization radius 1400
https-server authentication certificate 1401
ssh certificate-as-authorized-key 1402
ssh two-factor-authentication 1403

UDLD commands 1405
clear udld statistics 1405
show udld 1405
udld 1407
udld interval 1408
udld mode 1410
udld retries 1412

UFD (Uplink Failure Detection) commands 1414
debug ufd all 1414
delay 1414
links-to-disable 1416

links-to-monitor ... 1417
show capacities ufd ... 1418
show running-config ufd ... 1419
show-tech ufd ... 1420
show ufd ... 1421
ufd enable ... 1422
ufd session-id ... 1423

UDP commands ... 1425
ip forward-protocol udp ... 1425
ip udp-bcast-forward ... 1426
show ip forward-protocol udp ... 1426

User and group commands ... 1429
password complexity ... 1429
user ... 1433
user-group ... 1435
user management-interface ... 1439
user password ... 1441
service export-password ... 1442
show password-complexity ... 1443
show user-group ... 1444
show user information ... 1445
show user-list ... 1447
show user-list management-interface ... 1448

VLAN commands ... 1450
description ... 1450
vlan name ... 1450
show capacities-status vlan-count ... 1451
show capacities svi-count ... 1452
show capacities vlan-count ... 1453
show vlan ... 1453
show vlan port ... 1454
show vlan summary ... 1457
show vlan voice ... 1458
shutdown ... 1459
system vlan-client-presence-detect ... 1460
trunk-dynamic-vlan-include ... 1461
vlan ... 1461
vlan access ... 1463
vlan trunk allowed ... 1464
vlan trunk native ... 1465
vlan trunk native tag ... 1467
voice ... 1468

Zeroization commands ... 1469
erase all zeroize ... 1469

ZTP commands ... 1472
show ztp information ... 1472
ztp force provision ... 1476

Support and Other Resources ... 1478
Accessing HPE Aruba Networking Support ... 1478

Accessing Updates 1479
Warranty Information 1479
Regulatory Information 1479
Documentation Feedback 1479

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 Aruba switches on a network.

Applicable products

This document applies to the following products:

- HPE Aruba Networking 6000 Switch Series (R8N85A, R8N86A, R8N87A, R8N88A, R8N89A, R9Y03A)
- HPE Aruba Networking 6100 Switch Series (JL675A, JL676A, JL677A, JL678A, JL679A)

What's new in this release

Commands introduced or modified in 10.14.0001

Command	Description
arp ip	Replaced the **ipv4** parameter with the **ip** parameter. The**i pv4** parameter is deprecated.
clear arp	Replaced the **ipv4** parameter with the **ip** parameter. The **ipv4** parameter is deprecated.
clear dhcp-snooping binding	Replaced the **ipv4** parameter with the **ip** parameter. The **ipv4** parameter is deprecated.
dhcp-snooping ... show dhcp-snooping ... clear dhcp-snooping ...	The **dhcp*v4*-snooping**, **show dhcp*v4*-snooping**, and **clear dhcp*v4*-snooping** series of commands are deprecated, and are replaced with **dhcp-snooping**, **show dhcp-snooping** and **clear dhcp-snooping** commands with similarsyntax and functionality.
ip igmp snooping filter unknown mcast	Command that enables the avoidance of initial flooding of unknown multicast traffic on IGMP-snooping-enabled VLAN introduced on the 4100i, 6000, and 6100.
ipv6 mld snooping filter-unknown-mcast	Command that configures the unknown multicast to steal when the MLD snooping is enabled introduced on the 4100i, 6000, and 6100.
rate-limit	Replaced the **ipv4** parameter with the **ip** parameter. The **ipv4** parameter is deprecated.
show history	The **all-sessions** parameter is introduced.
show snmp community	The output of this command now displays an error message when the switch is in SNMPv3-only mode.
snmp-server community	Replaced the **ipv4** parameter with the **ip** parameter. Th e**ipv4** parameter is deprecated.

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
`example-text`	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: ■ *<example-text>* ■ <example-text> ■ *example-text* ■ *example-text*	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 6000 and 6100 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.

Chapter 2
Introduction to the AOS-CX CLI

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 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.

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>)#**

The switch prompt is truncated to 50 characters.

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 the 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
`example-text`	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: ■ *<example-text>* ■ <example-text> ■ *example-text* ■ *example-text*	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:

```
SVOS> boot

ServiceOS Information:
    Version:          PL.01.07.0004-internal
    Build Date:       2020-11-23 18:07:42 PST
    Build ID:         ServiceOS:PL.01.07.0004-internal:133137f635df:202011231807
    SHA:              133137f635dff5778bf3e109eb75825b68d64789

Boot Profiles:

0. Service OS Console
1. Primary Software Image [PL.10.06.0001]
2. Secondary Software Image [PL.10.08.0000-168-g3089099c34e6]

Select profile(primary):
```

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-FLENAME/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-FLENAME/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 eMMC 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

 ServiceOS Information:
    Version: PL.01.07.0004-internal
    Build Date: 2020-11-23 18:07:42 PST
    Build ID: ServiceOS:PL.01.07.0004-internal:133137f635df:202011231807
    SHA: 133137f635dff5778bf3e109eb75825b68d64789

################ 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

Loging the user out from the `SVOS>` prompt:

```
SVOS> exit

(C) Copyright 2024 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.

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.

ls

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

Description

This command lists directory contents.

Parameter	Description
<OPTIONS>	Specifies options for the command.
`-1`	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**.

Parameter	Description
`-t`	With **-l**, it shows a sort by **mtime**.
`-u`	With **-l**, sort by **atime**.
`-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.
`-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

Parameter	Description
	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 eMMC 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 `all` and `usb`.

Examples

Mounting all of the eMMC 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.

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
`[-f | -i | -R | -r]`	Selects the options for removing files or directories.
`-f`	Never prompt before removing files or directories.
`-i`	Always prompt before removing files or directories.
`-R | -r`	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
`-p`	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

Enablling 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 eMMC 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.

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.

On the 6000 and 6100 Switch Series, only the vrf named `default` is available. Replace any references to the `mgmt` or other VRFs with `default`.

ACL application

ACLs can be applied as follows:

ACL type Direction	IPv4+6 In	MAC In
L2 interface (port)	Yes	Yes
L2 LAG	Yes	Yes
VLAN	Yes	Yes
Control Plane (default VRF)	Yes	

The following match criteria is not supported. If this match criteria is attempted to be configured, an error message will be displayed and the action will not be completed.

```
TTL on IP ACLs
```

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                          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
------------------------------------------------------------------------------
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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
```

```
------------------------------------------------------------------------------
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                          ipv6
           1122.3344.5566/ffff.ffff.0000
           any
         2 permit                          any
           aaaa.bbbb.cccc
           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                          ipv6
            1122.3344.5566/ffff.ffff.0000
            any
          2 permit                          any
            aaaa.bbbb.cccc
            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                          ipv6
            1122.3344.5566/ffff.ffff.0000
            any
          2 permit                          any
            aaaa.bbbb.cccc
            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                          ipv6
            1122.3344.5566/ffff.ffff.0000
            any
          2 permit                          any
            aaaa.bbbb.cccc
            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 Classifiers Policy 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>}]}
  {any|<DST-IP-ADDRESS>[/{<PREFIX-LENGTH>|<SUBNET-MASK>}]}
  [dscp <DSCP-SPECIFIER>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>}]}
  [{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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>]  [fragment] [vlan <VLAN-ID>] [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>}]}
  {any|<DST-IP-ADDRESS>[/{<PREFIX-LENGTH>|<SUBNET-MASK>}]}
  [icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
  [dscp <DSCP-SPECIFIER>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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
<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.
<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>*[/{*<PREFIX-LENGTH>*|*<SUBNET-MASK>*}]}	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).
{any|*<DST-IP-ADDRESS>*[/{*<PREFIX-LENGTH>*|*<SUBNET-MASK>*}]}	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).
[{eq|gt|lt} *<PORT>*|range *<MIN-PORT>* *<MAX-PORT>*]	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

Parameter	Description
	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. **NOTE:** Upon application of the ACL, ACEs with L4 port ranges may consume more than one hardware entry.
`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.
`[icmp-type {echo|echo-reply|` *`<ICMP-TYPE-VALUE>`*`}]`	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.
`[icmp-code` *`<ICMP-CODE-VALUE>`*`]`	Specifies the ICMP code value. Range: 0 to 255.
`dscp` *`DSCP-SPECIFIER>`*	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

Parameter	Description
	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)
`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>*	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.
`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 both `permit` and `deny` 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 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                          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
           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
```

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                          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
           172.16.1.0/255.255.255.0
        20 Permit all TCP ephemeral ports
           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
```

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                           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
           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
```

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                           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
           172.16.1.0/255.255.255.0
        20 permit                          tcp
           172.16.2.0/255.255.0.0           >  1023
           any
        25 permit                          icmp
           172.16.2.0/255.255.0.0 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
```

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                          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
           172.16.1.0/255.255.255.0
        20 permit                          tcp
           172.16.2.0/255.255.0.0           >  1023
           any
        25 permit                          icmp
           172.17.1.0/255.255.0.0
        30 permit                          tcp
           172.26.1.0/255.255.255.0
           any
           dscp: AF11
           ack
           syn
        40 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
------------------------------------------------------------------------------
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
        25 permit                          icmp
           172.17.1.0/255.255.0.0
        30 permit                          tcp
           172.26.1.0/255.255.255.0
           any
           dscp: AF11
           ack
           syn
        40 deny                            any
           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                          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
           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
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
        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                          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
           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
           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 switch(config)# access-list ip MY_IP_ACL copy MY_
IP_ACL2
switch(config)# 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
        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                           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
```

Removing an IPv4 ACL:

```
switch(config)# no access-list ip MY_IP_ACL

switch(config)# 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_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
```

For more information on features that use this command, refer to the ACLs and Classifiers Policy 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>]}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]}
[dscp <DSCP-SPECIFIER>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>}]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]}
[{eq|gt|lt} <PORT>|range <MIN-PORT> <MAX-PORT>]
[urg] [ack] [psh] [rst] [syn] [fin] [established]
[dscp <DSCP-SPECIFIER>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>]}
{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]}
[icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}] [icmp-code <ICMP-CODE-VALUE>]
[dscp <DSCP-SPECIFIER>][ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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
<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.
<IP-PROTOCOL-NUM>	Specifies the protocol as its Internet Protocol number. For

Parameter	Description
	example, 2 corresponds to the IGMP protocol. Range: 0 to 255.
`{any|<SRC-IP-ADDRESS>[/<PREFIX-LENGTH>]}`	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.
`{any|<DST-IP-ADDRESS>[/<PREFIX-LENGTH>]}`	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.
`[{eq|gt|lt} <PORT>|range <MIN-PORT><MAX-PORT>]`	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. ▪ **lt *<PORT>*** - specifies any Layer 4 port less than the indicated port. ▪ **range *<MIN-PORT>* *<MAX-PORT>*** - specifies the Layer 4 port range. **NOTE:** Upon application of the ACL, ACEs with L4 port ranges may consume more than one hardware entry.
`[icmp-type {echo|echo-reply|<ICMP-TYPE-VALUE>}]`	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.
`[icmp-code <ICMP-CODE-VALUE>]`	Specifies the ICMP code value. Range: 0 to 255.
`dscp <DSCP-SPECIFIER>`	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

Parameter	Description
	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)
`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.
`vlan <VLAN-ID>`	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.
`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 both `permit` and `deny` 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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           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 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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
IPv6       MY_IPV6_ACL
        10 permit                          udp
           any
           2001::1/64
        20 permit                          tcp
           2001:2001::2:1                   >  1023
           any
        25 permit                          icmpv6
           2001::2:1/64
           any
        30 permit                          tcp
           2001:2011::1/64
           any
        40 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
        10 permit                          udp
           any
           2001::1/64
        20 permit                          tcp
           2001:2001::2:1                   >  1023
           any
        25 permit                          icmpv6
           2001::2:1/64
           any
        30 permit                          tcp
           2001:2011::1/64
           any
        40 deny                            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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           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

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
        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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
--------------------------------------------------------------------------------
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 Classifiers Policy 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 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
`default`	Resets the log timer to its default 300 seconds.
<INTERVAL>	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 both `permit` and `deny` 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                          L3 Protocol
```

```
            Source IP Address               Source L4 Port(s)
            Destination IP Address          Destination L4 Port(s)
            Additional Parameters
------------------------------------------------------------------------------
IPv4        MY_IP_ACL
         10 deny                            icmp
            1.1.1.1
            1.1.1.2
            Logging: enabled
            Hit-counts: enabled
```

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

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 Classifiers Policy 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|aarp|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 any. 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 any. You can optionally include the following: *<ETHERNET-MASK>* - The address bits to mask (xxxx.xxxx.xxxx).
{any|aarp|appletalk| ... |wake-on-lan|*<NUMERIC-ETHERTYPE>*	Specifics 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: ◦ aarp ◦ 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`	

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                          ipv6
           1122.3344.5566/ffff.ffff.0000
           any
        20 permit                          any
           aaaa.bbbb.cccc
           1111.2222.3333
           QoS Priority Code Point: 4
        30 permit                          appletalk
           any
           any
           VLAN: 40
        40 deny                            any
           any
           any
           Hit-counts: enabled
```

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                           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                           appletalk
           any
           any
           VLAN: 1
        40 deny                             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                           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                           appletalk
           any
           any
           VLAN: 1
        35 permit                           0xffee
           any
           aabb.cc11.1234
        40 deny                             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                          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                          appletalk
           any
           any
           VLAN: 1
        35 permit                          0xeeee
           any
           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                          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                          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                           EtherType
           Source MAC Address
           Destination MAC Address
           Additional Parameters
------------------------------------------------------------------------------
MAC        MY_MAC_ACL2
         1 permit                           ipv6
           1122.3344.5566/ffff.ffff.0000
           any
         2 permit                           any
           aaaa.bbbb.cccc
           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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config` The `access-list mac <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 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                          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
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                          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
```

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                          ipv6
            1122.3344.5566/ffff.ffff.0000
            any
          2 permit                          any
            aaaa.bbbb.cccc
            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 Classifiers Policy 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
`all|ip` *ACL-NAME*`>|ipv6` *<ACL-NAME>*`|mac` *<ACL-NAME>*	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 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
! 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

! 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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
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
------------------------------------------------------------------------------
IPv4       TEST_ACL
```

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

Related Commands

Command	Description
`vsx-sync acl-secure-update`	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 *Virtual Switching Extension (VSX) Guide* 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 Classifiers Policy 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)

```
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 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: `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 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 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_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)#
```

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

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

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

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

Command History

Release	Modification
10.12.1000	Egress support extended to 6000 and 6100 switch series for MAC ACLs.
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 L3 VNI)

Description

Parameter	Description
`ip|ipv6`	Specifies the ACL type: **ip** for IPv4 or **ipv6** for IPv6.
<ACL-NAME>	Specifies the ACL name.

Examples

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

Command History

Release	Modification
10.12.1000	Egress support extended to 6000 and 6100 switch series for MAC ACLs.
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.

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.
	Selects the outbound (egress) traffic direction. **NOTE:** For 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. Therefore, using the **apply access-list** command on a VLAN with an already-applied ACL of the same type, will replace the applied ACL.
- When an ACL is applied to a VLAN, it will create hardware entries on all stack members regardless of whether a VLAN member exists on any specific stack member.

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 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
```

Applying My_mac_ACL to egress traffic on VLAN 10:

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

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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.12.1000	Egress support extended to 6000 and 6100 switch series for MAC ACLs.
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] }
```

Description

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

Parameter	Description
`all`	Selects all ACLs.
`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 LAG).
`vlan` *<VLAN-ID>*	Specifies the VLAN.

Parameter	Description
`in`	Selects the inbound (ingress) traffic direction.
`out`	Selects the outbound (egress) traffic direction. **NOTE:** For 6000 and 6100 switch series, the outbound (egress) traffic direction is supported only for MAC ACLs.

Examples

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 My_mac_ACL applied to VLAN 10 (egress):

```
switch# clear access-list hitcounts mac My_mac_ACL vlan 10 out
```

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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.12.1000	Egress support extended to 6000 and 6100 switch series for MAC ACLs.
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 Classifiers Policy 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

Syntax that filters by ACLs applied to an interface, VLAN, or VNI:

```
show access-list [interface <IF-NAME>|vlan <VLAN-ID>] [ip|ipv6|mac]
                 [in|out] [commands] [configuration]
```

Syntax that filters by the named ACL:

```
show access-list [ip|ipv6|mac] [<ACL-NAME>] [commands] [configuration]
```

Description

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 to a specific interface (port or split port or LAG).
- The ACL applied to a specific VLAN.
- All IPv4 or IPv6 ACLs applied to interface VLANs.

Parameter	Description
`interface <IF-NAME>`	Specifies the interface name (port or LAG).
`vlan <VLAN-ID>`	Specifies the VLAN.
`ip|ipv6|mac`	Specifies the ACL type: ■ **ip** for IPv4, ■ **ipv6** for IPv6, or ■ **mac** for MAC.
`in`	Selects the inbound (ingress) traffic direction.
`out`	Selects the outbound (egress) traffic direction. **NOTE:** For 6000 and 6100 switch series, the outbound (egress) traffic direction is supported only for MAC ACLs.
<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.

Examples

Showing an IPv4 ACL:

```
switch# show access-list ip MY_ACL
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_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
           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                          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
           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
           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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
```

```
------------------------------------------------------------------------------
IPv6        MY_IPV6_ACL
         10 permit                          udp
            any
            2001::1/64
         20 permit                          tcp
            2001:2001::2:1/128               >  1023
            any
         30 permit                          tcp
            2001:2011::1/64
         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                          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 deny                            any
            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 pcp 4
    30 deny any any any count
```

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

Command History

Release	Modification
10.12.1000	Egress support extended to 6000 and 6100 switch series for MAC ACLs.
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 control-plane

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

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

Parameter	Description
	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.

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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
IPv4       My_ipv4_ACL
        10 permit                          udp
           any
           172.16.1.0/24
        20 permit                          tcp
           172.16.2.0/16                    >  1023
           any
        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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
IPv6       My_ipv6_ACL
        10 permit                          udp
           any
           2001::1/64
        20 permit                          tcp
           2001:2001::2:1/128               >  1023
           any
        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 Classifiers Policy 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

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

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.
`in`	Selects the inbound (ingress) traffic direction.
`out`	Selects the outbound (egress) traffic direction. **NOTE:** For 6000 and 6100 switch series, the outbound (egress) traffic direction is supported only for MAC ACLs.

Usage

- ACL hit counts are aggregated across all:
  - Physical interfaces to which the ACL is applied to on ingress.
  - VLANs to which the ACL is applied to on ingress.
- 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
```

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

Command History

Release	Modification
10.12.1000	Egress support extended to 6000 and 6100 switch series for MAC ACLs.
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>`

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.

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 Classifiers Policy 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 Classifiers Policy Guide for your switch model.

Related Commands

Command	Description
`access-list secure-update`	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	`config`	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 Aruba 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 Aruba-Central location.
`vrf` *<VRF>*	Specifies the VRF used to connect to Aruba-Central.

Usage

When the main and alternative Aruba Central server locations are specified, the switch attempts to connect to the main Aruba Central server. If there is connectivity failure with the main Aruba 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 Aruba 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 aruba-central.com location and VRF red:

```
switch(config-aruba-central)# location-override-alternative aruba-central.com vrf
red
switch(config-aruba-central)#
```

Example of a configuration with location only:

```
switch(config-aruba-central)# location-override-alternative aruba-central.com
switch(config-aruba-central)#
```

Example of removing the override configuration:

```
switch(config-aruba-central)# no location-override-alternative
switch(config-aruba-central)# location-override-alternative 10.0.0.1 vrf red
switch(config-aruba-central)# location-override-alternative 10.0.0.1:443 vrf red
switch(config-aruba-central)# location-override-alternative
2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf red
switch(config-aruba-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-aruba-central`	Administrators or local user group members with execution rights for this command.

show capacities

`show capacities <FEATURE>`

Description

Shows system capacities and their values for all features or a specific feature.

Parameter	Description
<FEATURE>	Specifies a feature. For example, **aaa**.

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 classifier-related capacities on the 4100i, 6000, or 6100:

```
switch# show capacities classifier
```

```
System Capacities: Filter Classifier
Capacities Name                                                                  Value
--------------------------------------------------------------------------------
--
Maximum number of Access Control Entries configurable in a system
4096
Maximum number of Access Control Lists configurable in a system
512
Maximum number of class entries configurable in a system
4096
Maximum number of classes configurable in a system
512
Maximum number of entries in an Access Control List
1024
Maximum number of entries in a class
1024
Maximum number of entries in a policy
64
Maximum number of classifier policies configurable in a system
512
Maximum number of policy entries configurable in a system
4096
```

```
Showing all available capacities on the 4100i, 6000, or 6100:
                switch# show capacities

System Capacities:
Capacities Name                                                                Value
--------------------------------------------------------------------------------
-
Maximum number of Access Control Entries configurable in a system             4096
Maximum number of Access Control Lists configurable in a system                512
Maximum number of class entries configurable in a system                      4096
Maximum number of classes configurable in a system                             512
Maximum number of entries in an Access Control List                           1024
Maximum number of entries in a class                                          1024
Maximum number of entries in a policy                                           64
Maximum number of classifier policies configurable in a system                 512
Maximum number of policy entries configurable in a system                     4096
Maximum number of clients supported for tracking the IP address in the system  128
Maximum number of dynamic VLANs that can be allowed using MVRP                 256
Maximum number of nexthops per IP ECMP group                                     1
Maximum number of IP neighbors (IPv4+IPv6) supported in the system            1024
Maximum number of IPv4 neighbors(# of ARP entries) supported in the system    1024
Maximum number of IPv6 neighbors(# of ND entries) supported in the system      512
Maximum number of L2 MAC addresses supported in the system                    8192
Maximum number of L3 Groups for IP Tunnels and ECMP Groups                       1
Maximum number of L3 Destinations for Routes, Nexthops in Tunnels and ECMP groups
 1024
Maximum number of configurable LAG ports                                         8
Maximum number of members supported by a LAG port                                8
Maximum number of VLANs across ports allowed in loop-protect                  3328
Maximum number of IGMP/MLD groups supported                                    512
Maximum number of IGMP/MLD snooping groups supported                           512
Maximum number of Mirror Sessions configurable in a system                       4
Maximum number of enabled Mirror Sessions in a system                            4
Maximum number of mstp instances configurable in a system                       16
Maximum number of Clients that can be authenticated on a port                   32
Maximum number of Device Profiles allowed to be created on the system            8
```

```
Maximum number of Port Access Roles allowed to be created on the system         32
Maximum number of MAC Address that can be authorized on a port                  32
Maximum number of Port Access Role VLAN IDs allowed to be created on the system 50
Maximum number of Port Access Role VLAN names allowed to be created on the system
   50
Maximum number of RBAC rules per user group                                   1024
Maximum number of RPVST VLANs configurable on the system                        16
Maximum number of RPVST VPORTs supported in a system                           512
Maximum number of SVIs supported in the system                                  16
Maximum number of routes (IPv4+IPv6) on the system                             512
Maximum number of IPv4 routes on the system                                    512
Maximum number of IPv6 routes on the system                                    512
Maximum number of VLANs supported in the system                                512
```

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 Classifiers Policy 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>`

Description

Shows system capacities status and their values for all features or a specific feature.

Parameter	Description
<FEATURE>	Specifies the feature, for example **aaa** for which to display capacities, values, and status. Required.

Examples

Showing the system capacities status for all features:

```
switch# show capacities-status
System Capacities Status
Capacities Status Name                                                          Value
Maximum
--------------------------------------------------------------------------------
----
Number of Access Control Entries currently configured                            0
4096
Number of Access Control Lists currently configured                              0
512
Number of class entries currently configured                                     0
4096
Number of classes currently configured                                           0
512
Number of policies currently configured                                          0
512
Number of policy entries currently configured                                    0
4096
Number of dynamic VLANs currently learnt using MVRP                              0
256
```

```
Number of IP neighbor (IPv4+IPv6) entries                                  1
1024
Number of IPv4 neighbor(ARP) entries                                       1
1024
Number of IPv6 neighbor(ND) entries                                        0
512
Number of L3 Groups for IP Tunnels and ECMP Groups currently configured    0
1
Number of L3 Destinations for Routes, Nexthops in ECMP groups and Tunnels
  currently configured                                                     0
1024
Number of Mirror Sessions currently configured                             0
4
Number of Mirror Sessions currently enabled                                0
4
Number of mstp instances currently configured                              0
16
Number of RPVST VLANs currently configured                                 0
16
Number of routes (IPv4+IPv6) currently configured                          1
512
Number of IPv4 routes currently configured                                 1
512
Number of IPv6 routes currently configured with prefix 0-64                0
512
Number of IPv6 routes currently configured with prefix 65-127              0
512
Number of VLANs currently configured                                       1
512
```

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 Classifiers Policy 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 resources

```
show resources
```

Description

Shows hardware resource consumption. Resource data is updated every 10 seconds.

Hardware resource consumption information is shown for:

- TCAM entries
- TCAM lookups
- Policers

Usage

```
  "Ingress IP Port ACL" = Ingress v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2) /  "Ingress IP Port ACL" = Ingress v4
Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2C(v2)/  "Ingress IP Port ACL" = Ingress
v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2C(v2) /  "Ingress IP Port ACL" = Ingress
v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2) /  "Ingress IP Port ACL" = Ingress v4
Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2C(v2)/  "Ingress IP Port ACL" = Ingress
v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
```

```
                        = 5 TCAM entriC(v2C(v2C(v2)/  "Ingress IP Port ACL" =
Ingress v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2) /  "Ingress IP Port ACL" = Ingress v4
Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2C(v2)/  "Ingress IP Port ACL" = Ingress
v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries/  "Ingress IP Port ACL" = Ingress v4 Port
ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entriC(v2C(v2C(v2)
```

```
MAC ACL    1
IPv4 ACL   1
IPv6 ACL   4
MAC Class  1
IPv4 Class 2
IPv6 Class 4
```

The widths for show resources can have features combined (IPv4 + IPv6) into one TCAM lookup. Therefore, the table widths for each ACL/classifier policy type are variable depending on what is applied. For example:

```
  "Ingress IP Port ACL" = Ingress v4 Port ACLs + Ingress v6 Port ACLs
                        = 1 TCAM entry + 4 TCAM entries
                        = 5 TCAM entries
```

Widths per feature are as follows:

```
IPv4 ACL   2
MAC ACL    2
IPv6 ACL   4
IPv4 Class 2
IPv6 Class 4
```

Examples

```
switch# show resources

Resource Usage:

Mod  Description
         Resource                                    Used Reserved    Free
-------------------------------------------------------------------------
1/1  Ingress IP Port ACL Lookup
         Ingress TCAM Entries                          20        0    5093
```

```
     Total
         Ingress Lookups                                1        0        4
         Egress Lookups                                 0        0        4
```

```
switch# show resources

Resource Usage:

Mod  Description
         Resource                                    Used     Free
-------------------------------------------------------------------------------
1/3  Total
         Ingress Lookups                               0        5
         Egress Lookups                                0        4
1/5  Total
         Ingress Lookups                               0        5
         Egress Lookups                                0        4
```

```
switch# show resources

Resource Usage:

Mod  Description
         Resource                                    Used Reserved    Free
-------------------------------------------------------------------------------
1/1  Total
         Ingress TCAM Entries                          0        0    5120
         Egress TCAM Entries                           0        0    2048
         Ingress Lookups                               0               9
         Egress Lookups                                0               4
         Ingress Policers                              0            2047
         Egress Policers                               0            2047
```

Showing hardware resource consumption on a 6100 switch:

```
switch# show resources
Resource Usage:
Mod  Description
         Resource                                    Used Reserved    Free
-------------------------------------------------------------------------------
1/1  Ingress IPv4 VLAN ACL Lookup
         Ingress TCAM Entries                          4      128
     Ingress IPv6 VLAN ACL Lookup
         Ingress TCAM Entries                          8      128
     Ingress IP CPURX Lookup
         Ingress TCAM Entries                        126      128
         Ingress Policers                             19
     Ingress IP Port Policy Lookup
         Ingress TCAM Entries                          2      128
     Ingress IP VLAN Policy Lookup
         Ingress TCAM Entries                         12      128
     Total
         Ingress TCAM Entries                        152      640    3448
         Ingress Lookups                               5               27
         Ingress Policers                             19            2029
```

```
switch# show resources 1/1
Resource Usage:
Mod  Description
         Resource                              Width    Used Reserved    Free
-------------------------------------------------------------------------------
1/1  Ingress IPv4 Port ACL
         High-Capacity TCAM/LPM Entries        2       0   262144
     MAC Control Plane Policing
         TCAM Entries                          2      16      256
     IPv4 Control Plane Policing
         TCAM Entries                          2      70      256
     IPv6 Control Plane Policing
         TCAM Entries                          2      72        *
     IPv4 Unicast Route
         High-Capacity TCAM/LPM Entries        1       0   131072
     IPv6 Unicast Route
         High-Capacity TCAM/LPM Entries        2       0   262144
     IPv4 Multicast Route
         High-Capacity TCAM/LPM Entries        2       0    65536
     IPv6 Multicast Route
         High-Capacity TCAM/LPM Entries        4       0    65536
     Total
         TCAM Entries                                158      512   49664
         High-Capacity TCAM/LPM Entries                0   786432  258048
         Policers                                      0           65536
         Ingress L4 Port Ranges                        0              24
* This feature shares reserved resources with the preceding feature.
```

```
switch# show resources
Resource Usage:
Mod  Description
         Resource                              Width    Used Reserved    Free
-------------------------------------------------------------------------------
1/1  Ingress IPv4 Port ACL
         Ingress TCAM Entries                  1       2     2048
     Ingress MAC+IPv4 Port Policy
         Ingress TCAM Entries                  2       8     2048
     Ingress Control Plane Policing
         Ingress TCAM Entries                  2     152     1024
     Egress Control Plane Policing
         Egress TCAM Entries                   2      84      256
     Total
         Ingress TCAM Entries                        162     5120   11264
         Egress TCAM Entries                          84      256     768
         Policers                                      0           16384
         Ingress L4 Port Ranges                        0              32
```

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 inspection

```
arp inspection
```

Description

Enables Dynamic ARP inspection on the current VLAN, which means that ARP packets received from untrusted interfaces are discarded if they have an Invalid IP-to-MAC address binding.

The **no** form of this command disables Dynamic ARP Inspection on the VLAN.

Examples

Enabling dynamic ARP inspection:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# arp inspection
```

Disabling dynamic ARP inspection:

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# no arp inspection
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	config-vlan-*<VLAN-ID>*	Administrators or local user group members with execution rights for this command.

arp inspection trust

```
arp inspection trust
no arp inspection trust
```

Description

Configures the interface as a trusted. All interfaces are untrusted by default.

The **no** form of this command returns the interface to the default state (untrusted).

Example

Setting an interface as trusted:

```
switch(config-if)# arp inspection trust
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

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 VLAN**10**:

```
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 Aruba 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: **vlan 2**.

Parameter	Description
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 he **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 vlan 2
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	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.

debug arp-security

```
debug arp-security <LOG-CATEGORY> [severity <LEVEL>]
no debug arp-security [<LOG-CATEGORY>] [severity <LEVEL>]
```

Description

Enables ARP security debug logs. If <SEVERITY> is omitted, all severities are logged.

The **no** form of this command disables ARP security debug logs.

Parameter	Description
<LOG-CATEGORY>	Selects the ARP security debug log category. Available categories are: ■ **all**: Selects all ARP security debug log categories. ■ **config**: Selects the ARP security config debug log category. ■ **inspection**: Selects the ARP security inspection debug log category. ■ **packet**: Selects the ARP security packet debug log category.
`severity <LEVEL>`	Specifies how to filter the ARP security debug logging by setting the minimum severity level for which debug logging will be performed. The selected severity level and all severities above (more severe) will be included in the logging. ■ **emerg**: Sets ARP security debug log filtering to Emergency only. ■ **alert**: Sets ARP security debug log filtering to Alert and above. ■ **critical**: Sets ARP security debug log filtering to Critical and above. ■ **error**: Sets ARP security debug log filtering to Error and above. ■ **warning**: Sets ARP security debug log filtering to Warning and above. ■ **notice**: Sets ARP security debug log filtering to Notice and above. ■ **info**: Sets ARP security debug log filtering to Info and above. ■ **debug**: Sets ARP security debug log filtering to all severities.

Examples

Enable ARP security debug logging for all categories and all severities:

```
switch# debug arp-security all
```

Enable ARP security config debug log for severity level Error and above:

```
switch# debug arp-security config severity error
```

Enable ARP security inspection debug log for severity level Notice and above:

```
switch# debug arp-security inspection severity notice
```

Enable ARP security debug packet for severity level Critical and above:

```
switch# debug arp-security packet severity critical
```

Enable ARP security debug logging for all categories and severity level Alert and above:

```
switch# debug arp-security all severity alert
```

Disable ARP security debug logging:

```
switch# no debug arp-security
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 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 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 **vlan 2**.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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`

Description

Shows the entries in the ARP (Address Resolution Protocol) table.

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 inspection interface

`show arp inspection interface [<IFNAME>] [vlan <VLAN-ID>]`

Description

Shows the current configuration of dynamic ARP inspection on an interface.

Parameter	Description
<IFNAME>	Specifies the interface.
<VLAN-ID>	Specifies the VLAN ID. Range: 1 to 4094.

Examples

Showing current configuration of dynamic ARP inspection on all interfaces:

```
switch# show arp inspection interface

-------------------------------------------------------------------------------
Interface           Trust-State
-------------------------------------------------------------------------------
1/1/1               Untrusted
-------------------------------------------------------------------------------
```

Showing current configuration of dynamic ARP inspection on a particular interface:

```
switch# show arp inspection interface 1/1/1

-------------------------------------------------------------------------------
Interface           Trust-State
-------------------------------------------------------------------------------
1/1/1               Untrusted
-------------------------------------------------------------------------------
```

Showing current configuration of dynamic ARP inspection on interface VLAN 2:

```
switch# show arp inspection interface vlan 2

------------------------------------------------------------------
Interface           Trust-State
------------------------------------------------------------------
vlan2               Trusted
------------------------------------------------------------------
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 inspection statistics

`show arp inspection statistics vlan [<VLAN-ID>]`

Description

Shows statistics about forwarded and dropped ARP packets. When *<VLAN-ID>* is not specified, information is shown for all configured VLANs.

Parameter	Description
<VLAN-ID>	Specifies the VLAN ID or range of IDs separated by a dash "-". Range: 1 to 4094.

Examples

Showing ARP packet statistics for a range of VLANs:

```
switch# show arp inspection statistics vlan 1-100

------------------------------------------------------------------
VLAN    Name              Forwarded           Dropped
------------------------------------------------------------------
1       DEFAULT_VLAN_1    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
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 inspection vlan

`show arp inspection vlan [<VLAN-ID>]`

Description

Shows the current configuration of dynamic ARP inspection on a VLAN. When <*VLAN-ID*> is not specified, information is shown for all configured VLANs.

Parameter	Description
<VLAN-ID>	Specifies the VLAN ID or range of IDs separated by a dash "-". Range: 1 to 4094.

Examples

Showing dynamic ARP configuration for all VLANs:

```
switch# show arp inspection vlan
------------------------------------------------------------------
VLAN   Name              ARP Inspection
------------------------------------------------------------------
1      DEFAULT_VLAN_1    -
100    VLAN100           -
200    VLAN200           Enabled
------------------------------------------------------------------
```

Showing dynamic ARP configuration for a particular VLAN:

```
switch# show arp inspection vlan 1
------------------------------------------------------------------
VLAN   Name              ARP Inspection
------------------------------------------------------------------
1      DEFAULT_VLAN_1    -
------------------------------------------------------------------
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 state

```
show arp state {all | failed | incomplete | permanent | reachable | stale}
```

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 `failed` state. The neighbor might have been deleted.
`incomplete`	Shows the ARP cache entries that are in `incomplete` 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 `permanent` 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 `reachable` state, meaning that the neighbor is known to have been reachable recently.
`stale`	Shows ARP cache entries that are in `stale` state. ARP cache entries are in the `stale` 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.

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>]`

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.

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>]`

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 (for example, `1/3/1`).

Examples

Showing ARP timeout information for a VLAN:

```
switch# show arp timeout vlan2
Port             VRF                                 Timeout
-------------------------------------------------------------
vlan2            default                             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 arp vrf

`show arp {all-vrfs | vrf <VRF-NAME>}`

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.

Examples

Showing ARP entries for VRF **vrf1**.

```
switch# show arp vrf vrf1

IPv4 Address     MAC                Port         Physical Port              State
    VRF
-------------------------------------------------------------------------------
------------
100.1.250.50     00:50:56:8d:44:13  vlan1001     1/1/2
reachable  vrf1
100.2.250.60     00:50:56:8d:45:63  vlan1002     vxlan1(1920:1680:1:1::2)
permanent  vrf1

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>}`

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
`all-vrfs`	Specifies all VRFs.
`vrf <VRF-NAME>`	Specifies the name of a VRF. Length: 1 to 32 alphanumeric characters.

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}`

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 `failed` state. The neighbor might have been deleted. Set the neighbor to be unreachable.
`incomplete`	Shows ARP cache entries that are in `incomplete` 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 `permanent` state.
`reachable`	Shows ARP cache entries that are in `reachable` state, meaning that the neighbor is known to have been reachable recently.
`stale`	Shows ARP cache entries that are in `stale` state. ARP cache entries are in the `stale` 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.

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.

show tech arp-security

```
show tech arp-security
```

Description

Shows the output of these three commands:

- **show arp inspection statistics vlan**
- **show arp inspection vlan**
- **show arp inspection interface**

Examples

Showing the output of the three ARP security show commands:

```
switch(config-if)# show tech arp-security
=====================================================
Show Tech executed on Mon Nov 28  09:53:54 2019
=====================================================
=====================================================
[Begin] Feature arp-security
=====================================================


*********************************
Command : show arp inspection statistics vlan
*********************************

-------------------------------------------------------------------
VLAN    Name              Forwarded           Dropped
-------------------------------------------------------------------
1       DEFAULT_VLAN_1    0                   0
200     VLAN200           0                   0
-------------------------------------------------------------------

*********************************
Command : show arp inspection vlan
*********************************

-------------------------------------------------------------------
VLAN    Name              ARP-Inspection
-------------------------------------------------------------------
1       DEFAULT_VLAN_1    -
200     VLAN200           Enabled
-------------------------------------------------------------------

*********************************
Command : show arp inspection interface
*********************************

-------------------------------------------------------------------------------
Interface           Trust-State
```

```
--------------------------------------------------------------------------------
1/1/1               Untrusted
lag100              Trusted
--------------------------------------------------------------------------------
======================================================
[End] Feature arp-security
======================================================


======================================================
Show Tech commands executed successfully
======================================================
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced on the 6000, 6100 Switch Series

Command Information

Platforms	Command context	Authority
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

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}`

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.

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.

boot set-default

```
boot set-default {primary | secondary}
```

Description

Sets the default operating system image to use when the system is booted.

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
`primary`	Selects the primary operating system image for this reboot and sets the configured default operating system image to **primary** for future reboots.
secondary	Selects the secondary operating system image for this reboot and sets the configured default operating system image to **secondary** for future reboots.
`serviceos`	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
`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 **show boot-history** command shows the number of seconds the module has been running on the current software.
`<Timestamp>: boot reason`	For previous boot operations, the **show boot-history** 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: ■ ***<DAEMON-NAME>* crash**: The daemon identified by *<DAEMON-NAME>* caused the module to boot. ■ **Kernel crash**: The operating system software associated with the module caused the module to boot. ■ **Uncontrolled reboot**: The reason for the reboot is not known. ■ **Reboot requested through database**: The reboot occurred because of a request made through the CLI or other API.

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
```

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.

diag cable-diagnostic

```
diag cable-diagnostic
   test <IF-NAME>
   show <IF-NAME>
   clear <IF-NAME>
```

Description

Provides information about the cable health after running a diagnostic test on an interface.

If you run a new cable diagnostic command when a cable diagnostic is in progress for the interface, the new cable diagnostic command fails to execute. In such a scenario, an error message is displayed.

On executing a cable diagnostic test command, it automatically clears the old test results before the new test starts.

Parameter	Description
<IF-NAME>	Specifies the name of the interface.
`test` *<IF-NAME>*	Runs a cable diagnostic test on an interface.
`show` *<IF-NAME>*	Displays the diagnostic test result for an interface.
`clear` *<IF-NAME>*	Clears the cable diagnostic test results for an interface.

Examples

The following example displays running a cable diagnostic test on interface `1/3/1`:

```
switch# diag cable-diagnostic test 1/3/1
This command will cause a loss of link on the port under test and will take
several seconds to complete.
Continue (y/n)? y
```

The following example displays the error message on executing a cable diagnostic command while the current diagnostic test is in progress:

```
switch# diag cable-diagnostic test 1/3/1
A cable diagnostic test for interface 1/3/1 is already in progress.
```

The following example displays the error message when cable diagnostic test is requested for an unsupported port:

```
switch# diag cable-diagnostic test 1/3/1
Cable diagnostic is not supported on interface 1/3/1.
```

The following examples display the cable diagnostic test result for 1GbT interface:

```
switch# diag cable-diagnostic show 1/3/1
                          Cable        Impedance   Distance*   MDI
Interface        Pinout   Status       (Ohms)      (Meters)    Mode
-------------------------------------------------------------------
1/3/1            1-2      good         85-115       10 +/- 10  mdi
(1GbT)           3-6      good         85-115       10 +/- 10  mdi
                 4-5      good         85-115        5 +/- 10  mdi
                 7-8      good         85-115        3 +/- 10  mdi

* Full cable length for good cables or distance to fault for faulty cables.

Cable status legend (1GbT):

Cable        Impedance
Status       (Ohms)     Description
-----------------------------------------------------------------
good         85-115     No cable faults found
open         >115       Open circuit detected
intra-short  <85        Short circuit within the same wire pair
inter-short  <85        Short circuit with another wire pair
high-imp     >115       Cable impedance higher than expected
low-imp      <85        Cable impedance lower than expected
unknown      --         Cable test inconclusive
```

The following examples display the cable diagnostic test result for 5G-SmartRate interface:

```
switch# diag cable-diagnostic show 1/1/20
                          Cable        Impedance   Distance*   MDI
Interface        Pinout   Status       (Ohms)      (Meters)    Mode
-------------------------------------------------------------------
1/1/20           1-2      good         85-115         --       mdi
(5G-SmartRate)   3-6      open         >300         4 +/- 5    mdi
                 4-5      open         >300         4 +/- 5    mdi
                 7-8      high-imp     >115         3 +/- 5    mdi

* Full cable length for good cables or distance to fault for faulty cables.

Cable status legend (5G-SmartRate):

Cable        Impedance
Status       (Ohms)     Description
-----------------------------------------------------------------
good         85-115     No cable faults found
open         >300       Open circuit detected
intra-short  <30        Short circuit within the same wire pair
inter-short  <30        Short circuit with another wire pair
high-imp     >115       Cable impedance higher than expected
low-imp      <85        Cable impedance lower than expected
unknown      --         Cable test inconclusive
```

The following example displays the error message when you execute a cable diagnostic command while the current diagnostic test is in progress:

```
switch# diag cable-diagnostic show 1/3/1
A cable diagnostic test for interface 1/3/1 is currently in progress.
```

The following example displays the error message when cable diagnostic test result is not available:

```
switch# diag cable-diagnostic show 1/3/1
Cable diagnostic test results for interface 1/3/1 are not available.
```

The following example clears the cable diagnostic test results for the specified interface:

```
switch# diag cable-diagnostic clear 1/3/1
```

The following example displays the error message when you execute a cable diagnostic command while the current diagnostic test is in progress:

```
switch# diag cable-diagnostic clear 1/3/1
A cable diagnostic test for interface 1/3/1 is currently in progress.
```

Running a cable diagnostic test will result in a brief interruption in connectivity on all tested ports.

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
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

aaa authentication port-access captive-portal-profile

```
aaa authentication port-access captive-portal-profile <PROFILE-NAME>
no aaa authentication port-access captive-portal-profile <PROFILE-NAME>
```

Description

Creates the specified captive portal profile (if it does not yet exist) and then enters its context. For existing captive portal profiles, this command enters the context of the specified captive portal profile.

The **no** form of this command deletes the specified captive portal profile.

Parameter	Description
<PROFILE-NAME>	Specifies the captive portal profile name. From 2 to 64 characters.

Examples

Creating a captive portal profile named `employee` and entering its context for additional configuration:

```
switch(config)# aaa authentication port-access captive-portal-profile employee
switch(config-captive-portal)# url http://1.1.1.1/employee/captiveportal.php
switch(config-captive-portal)#
switch(config-captive-portal)# url-hash-key plaintext cjQrJ9#$erty
switch(config-captive-portal)#
switch(config-captive-portal)# exit
switch(config)#
```

Deleting the captive portal profile named `employee`:

```
switch(config)# no aaa authentication port-access captive-portal-profile employee
switch(config)#
```

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

Command History

Release	Modification
10.09.1000	Added support for the 4100i, 6000, 6100.

Command Information

Platforms	Command context	Authority
6000 6100	config	Administrators or local user group members with execution rights for this command.

show port-access captive-portal-profile

```
show port-access captive-portal-profile [name <PROFILE-NAME>]
```

Description

Shows the configuration information for all captive portal profiles or a particular captive portal profile.

Parameter	Description
<PROFILE-NAME>	Specifies the captive portal profile name. From 2 to 64 characters.

Example

Showing IPv4 local captive portal profile configuration information:

```
switch# show port-access captive-portal-profile name employee

Captive Portal Profile Configuration

    Name                        : employee
    Type                        : local
    URL                         : http://1.1.1.1/employee/captiveportal.php
    URL Hash Key                : SWNGWyMeYubHPDgVIirpEUwNK5Uf+r1vmhBIncQPw1Y=
```

Showing IPv6 local captive portal profile configuration information:

```
switch# show port-access captive-portal-profile name CP6

Captive Portal Profile Configuration

    Name                        : CP6
    Type                        : local
    URL                         : https://[2000::3]/guest/captive_portal.php
    URL Hash Key                : SWNGWyMeYubHPDgVIirpEUwNK5Uf+r1vmhBIncQPw1Y=
```

Showing IPv6 DUR captive portal profile configuration information (a DUR (Downloadable User Role) is not available on the 6000, 6100 Switch Series):

```
switch# show port-access captive-portal-profile name CP6_DUR_GUEST_ROLE

Captive Portal Profile Configuration

    Name                        : CP6_DUR_GUEST_ROLE
    Type                        : downloaded
    URL                         : https://[2030:1::40]/guest/captive_portal_2.php
```

Showing IPv6 RADIUS VSA captive portal profile configuration information:

```
switch# show port-access captive-portal-profile name RADIUS_2259748436

Captive Portal Profile Configuration

    Name                        : RADIUS_2259748436
    Type                        : radius
    URL                         : https://[2030:1::40]/guest/captive_portal_2.php
```

Showing all captive portal profile configuration information (DUR (Downloadable User Role) is not available on the 6000, 6100 Switch Series):

```
switch# show port-access captive-portal-profile

Captive Portal Profile Configuration

    Name                        : CP6
    Type                        : local
    URL                         : https://[2000::3]/guest/captive_portal.php
    URL Hash Key                : SWNGWyMeYubHPDgVIirpEUwNK5Uf+r1vmhBIncQPw1Y=

    Name                        : CP6_DUR_GUEST_ROLE
    Type                        : downloaded
    URL                         : https://[2030:1::40]/guest/captive_portal_2.php

    Name                        : RADIUS_2259748436
    Type                        : radius
    URL                         : https://[2030:1::40]/guest/captive_portal_2.php
```

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

Command History

Release	Modification
10.09.1000	Added support for the 4100i, 6000, 6100.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

url

```
url <URL>
no url
```

Description

Within the captive portal context, defines the captive portal URL.

The **no** form of this command deletes the captive portal URL.

Parameter	Description
<URL>	Specifies the captive portal URL as an IPv4 or IPv6 address or a fully-qualified domain name. Up to 1024 characters.

Examples

Creating a captive portal profile named `employee` and then setting its IPv4 redirect URL:

```
switch(config)# aaa authentication port-access captive-portal-profile employee
switch(config-captive-portal)# url http://1.1.1.1/employee/captiveportal.php
switch(config-captive-portal)#
switch(config-captive-portal)# exit
switch(config)#
```

Entering the captive portal profile `employee` and then deleting its URL:

```
switch(config)# aaa authentication port-access captive-portal-profile employee
switch(config-captive-portal)# no url
switch(config-captive-portal)#
switch(config-captive-portal)# exit
switch(config)#
```

Creating a captive portal profile named `CP6` and then setting its IPv6 redirect URL:

```
switch(config)# aaa authentication port-access captive-portal-profile CP6
switch(config-captive-portal)# url https://[2000::3]/guest/captive_portal.php
switch(config-captive-portal)#
switch(config-captive-portal)# exit
switch(config)#
```

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

Command History

Release	Modification
10.09.1000	Added support for the 4100i, 6000, 6100.

Command Information

Platforms	Command context	Authority
6000 6100	`config-captive-portal`	Administrators or local user group members with execution rights for this command.

url-hash-key

```
url-hash-key [{plaintext | ciphertext} <HASH-KEY>]
no url-hash-key
```

Description

Within the captive portal context, defines the captive portal URL hash key.

When this command is entered without parameters, plaintext hash key prompting occurs upon pressing Enter. The entered hash key characters are masked with asterisks.

The **no** form of this command deletes the captive portal URL hash key.

Parameter	Description
`{plaintext | ciphertext}`	Selects the URL hash key type as either `plaintext` or `ciphertext`.
<HASH-KEY>	Specifies the captive portal URL hash key. Up to 128 characters.

Examples

Creating a captive portal profile named `employee` and then setting its URL and URL hash key:

```
switch(config)# aaa authentication port-access captive-portal-profile employee
switch(config-captive-portal)# url http://1.1.1.1/employee/captiveportal.php
switch(config-captive-portal)#
switch(config-captive-portal)# url-hash-key plaintext cjQrJ9#$erty
switch(config-captive-portal)#
```

Creating a captive portal profile named `guest` and then setting its URL and entering the URL hash key when prompted:

```
switch(config)# aaa authentication port-access captive-portal-profile guest
switch(config-captive-portal)# url http://1.1.1.1/guest/captiveportal.php
switch(config-captive-portal)#
switch(config-captive-portal)# url-hash-key
Enter the URL Hash-Key: ****
Re-Enter the URL Hash-Key: ****
switch(config-captive-portal)#
```

Entering the captive portal profile `employee` and then deleting its URL hash key:

```
switch(config)# aaa authentication port-access captive-portal-profile employee
switch(config-captive-portal)# no url-hash-key
switch(config-captive-portal)#
```

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

Command History

Release	Modification
10.09.1000	Added support for the 4100i, 6000, 6100.

Command Information

Platforms	Command context	Authority
6000 6100	`config-captive-portal`	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` `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: **member/slot/port**.

Examples

Showing all CDP neighbor information:

```
switch(config)# show cdp neighbor-info
Total Neighbor Entries  : 1
Port        Device ID                Platform                 Capability
-------------------------------------------------------------------------
1/1/1       Aruba-3810M-24G-1-slot... Aruba 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           : Aruba-3810M-24G-1-slot(70106f-867800)
Address             : 127.0.0.1
Platform            : Aruba 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}
```

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.

Usability

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.

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#
```

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

```
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
`timeout <TIMEOUT>`	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
<OLD-CHECKPOINT-NAME>	Specifies the name of an existing checkpoint to be renamed.
<NEW-CHECKPOINT-NAME>	Specifies the new name for the checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-). **NOTE:** Do not start the checkpoint name with **CPC** 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
<CHECKPOINT-NAME>	Specifies a checkpoint name.
startup-config	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
<CHECKPOINT-NAME>	Specifies the name of a checkpoint.

<REMOTE-URL>	Specifies the remote destination and filename using the syntax:
	TFTP format:
	`tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME>`
	SFTP format:
	`sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME>`
	SCP format:
	`scp://USER@{IP|HOST}[:PORT]/FILE`

`vrf` *<VRF-NAME>*	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
<CHECKPOINT-NAME>	Specifies the name of the checkpoint to copy. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-).
<STORAGE-URL>>	Specifies the name of the target file on the USB drive using the following syntax: `usb:/<FILE>` 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
<REMOTE-URL>	Specifies a remote file using the following syntax: **TFTP format:**

Parameter	Description

	`tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME>`
	SFTP format:
	`sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME>`
	SCP format:
	`scp://USER@{IP|HOST}[:PORT]/FILE`

`<CHECKPOINT-NAME>`	Specifies the name of the target checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-). Required. **NOTE:** Do not start the checkpoint name with `CPC` because it is used for system-generated checkpoints.
`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*> {running-config | startup-config}

`copy <REMOTE-URL> {running-config | startup-config } [vrf <VRF-NAME>]`

Description

Copies a remote file containing a switch configuration to the running configuration or to the startup configuration.

Parameter	Description

<REMOTE-URL>	Specifies a remote file with the following syntax:
	TFTP format:
	`tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME>`
	SFTP format:
	`sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME>`
	SCP format:
	`scp://USER@{IP|HOST}[:PORT]/FILE`

`{running-config | startup-config}`	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.
`vrf <VRF-NAME>`	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
10.07 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
`startup-config`	Specifies that the startup configuration receives a copy of the running configuration.
`checkpoint <CHECKPOINT-NAME>`	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.

Parameter	Description
	NOTE: Do not start the checkpoint name with **CPC** 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:

Parameter	Description

	TFTP format:
	`tftp://<IP-ADDR>[:<PORT-NUM>]`
	`[;blocksize=<Value>]/<FILENAME>`
	SFTP format:
	`sftp://<USERNAME>@<IP-ADDR>`
	`[:<PORT-NUM>]/<FILENAME>`
	SCP format:
	`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: **usb:/*<file>***
`{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: **usb:/*<FILE>***
`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. **NOTE:** Do not start the checkpoint name with **CPC** 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 all|daemon <daemon-name> |kernel|vsf`	Erase one of the following sets of core-dump files: ■ all: Erase all core-dump files. ■ daemon <daemon-name>: Erase daemon core-dump files. ■ kerne:l Erase the kernel core-dump. ■
startup-config	Specifies the startup configuration.
all	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
```

```
AQBapQjwipebv36io0jFfde7ZzrHckncal1D+3n8XFTZKQdmYgAAADEtYOeHSme93xzdD0uz6Vr9Kl+XBz
B+2GB0UBxSF7rvgN2x8KSgkqv7iqXVQ0Te6LkSMnH4BdNaT3Bf25qyvOqmr4YakO1V3rg8zAOADkPktQD8
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 `show checkpoint list all` is replaced with `show checkpoint`.
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
<START-DATE>	Specifies the starting date for the range of saved checkpoints to show. Format: **YYYY-MM-DD**.
<END-DATE>	Specifies the endingdate for the range of saved checkpoints to show. Format: **YYYY-MM-DD**.

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 `show checkpoint list date <START-DATE> <END-DATE>` is replaced with `show checkpoint date <START-DATE> <END-DATE>`

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 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:

Policy type Direction	IPv4 In	IPv6 In
L2 interface (port)	Yes	Yes
L2 LAG	Yes	Yes
VLAN	Yes	Yes

Port policies and port-access client policies cannot be configured at the same time.

apply policy (config-if, config-lag-if, config-vlan)

Context config-if, config-lag-if:

```
apply policy <POLICY-NAME> {in} [per-interface]
no apply policy <POLICY-NAME> {in} [per-interface]
```

Context config-vlan:

```
apply policy <POLICY-NAME> in
no apply policy <POLICY-NAME> in
```

Description

Applies a policy to the current physical interface port or LAG or VLAN context.

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.
`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)

- 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 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 multiple VLANs (ingress):

```
switch(config)# vlan 10,20
switch(config-vlan-<10,20>)# apply policy MY_POLICY7 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
```

For more information on features that use this command, refer to the ACLs and Classifiers Policy 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`
	`config-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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

class copy

`class {ip|ipv6} <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} *<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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
------------------------------------------------------------------------------
IPv6       MY_IPV6_CLASS
         2 ignore                          udp
           any
```

```
            any
--------------------------------------------------------------------------------
IPv6        MY_IPV6_CLASS2
          2 ignore                          udp
            any
            any
```

For more information on features that use this command, refer to the ACLs and Classifiers Policy 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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>]  [fragment] [vlan <VLAN-ID>] [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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
[tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>* `[/{`*<PREFIX-LENGTH>*`|`*<SUBNET-MASK>*`}]}`	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).
`{any|`*<DST-IP-ADDRESS>* `[/{`*<PREFIX-LENGTH>*`|`*<SUBNET-MASK>*`}]}`	Specifies the destination IPv4 address. ■ **any** - specifies any destination IPv4 address. ■ **<DST-IP-ADDRESS>** - specifies the destination IPv4 host address. ◦ **<PREFIX-LENGTH>** - specifies the

Parameter	Description
	address bits to mask (CIDR subnet mask notation). Range: 1 to 32. ◦ **<SUBNET-MASK>** - specifies the address bits to mask (dotted decimal notation).
`[{eq|gt|lt} <PORT>|range <MIN-PORT><MAX-PORT>]`	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. ■ **lt <PORT>** - specifies any Layer 4 port less than the indicated port. ■ **range *<MIN-PORT>* *<MAX-PORT>*** - specifies the Layer 4 port range.
`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>`	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)

Parameter	Description
	▪ **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: Realtime) ▪ **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)
`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>`	Specifies VLAN tag to match on. 802.1Q VLAN ID. **NOTE:** 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.
`[<SEQUENCE-NUMBER>] comment <TEXT-STRING>`	Adds a comment to a class entry. The **no** 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.

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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
-------------------------------------------------------------------------------
IPv4       MY_IP_CLASS
        10 match                           icmp
           any
           any
        20 ignore                          udp
           any
           any
        30 match                           tcp
           192.168.0.1
           192.168.0.2
```

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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
-------------------------------------------------------------------------------
IPv4       MY_IP_CLASS
        10 match                           icmp
           any
           any
        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                            icmp
           any
           any
        20 ignore                           udp
           any
           any
        30 match                            tcp
           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                            icmp
           any
           any
        20 ignore                           udp
           any
           any
        30 match                            tcp
           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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
-------------------------------------------------------------------------------
IPv4       MY_IP_CLASS
       20  ignore                          udp
           any
           any
       30  match                           tcp
           192.168.0.1
           192.168.0.2
```

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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config` **The class ip <CLASS-NAME> command takes you into the config-class-ipconfig-class-ip context where you enter the class entries.**	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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>]  [fragment] [vlan <VLAN-ID>] [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>] [ip-precedence <IP-PRECEDENCE-VALUE>]
  [tos <TOS-VALUE>] [fragment] [vlan <VLAN-ID>] [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>*`[/ { `*<PREFIX-LENGTH>*`|`*<SUBNET-MASK>*`}]}`	Specifies the source IPv6 address. ■ **any** - specifies any source IPv6 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).
`{any|`*<DST-IP-ADDRESS>*`[/ { `*<PREFIX-LENGTH>*`|`*<SUBNET-MASK>*`}]}`	Specifies the destination IPv4 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 32. ◦ **<SUBNET-MASK>** - specifies the address bits to mask (dotted decimal notation).
`[{eq|gt|lt}` *<PORT>*`|range` *<MIN-PORT><MAX-PORT>*`]`	Specifies the port or port range. Port numbers are in the range of 0 to 65535. ■ **eq <PORT>** - specifies the Layer 4 port.

Parameter	Description
	▪ **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.
`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>*	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)

Parameter	Description
	■ **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)
`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>`	Specifies VLAN tag to match on. 802.1Q VLAN ID. **NOTE:** 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.
`[<SEQUENCE-NUMBER>] comment <TEXT-STRING>`	Adds a comment to a class entry. The **no** 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.

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                          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

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
```

Replacing an IPv6 class entry in an existing IPv6 class:

```
switch(config)# class ipv6 MY_IPV6_CLASS
switch(config-class-ipv6)# 10 match any any 1020::
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                           any
           any
           1020::
        20 ignore                          udp
           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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
```

```
           Additional Parameters
------------------------------------------------------------------------------
IPv6       MY_IPV6_CLASS
        20 ignore                          udp
           any
           any
```

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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config` The **class ipv6 <CLASS-NAME>** command takes you into the **config-class-ipv6** command context where you enter the class entries.	Administrators or local user group members with execution rights for this command.

class resequence

`class {ip|ipv6} <CLASS-NAME> resequence <STARTING-SEQUENCE-NUMBER> <INCREMENT>`

bDescription

Resequence numering in an IPv4, or IPv6 class.

Parameter	Description
{ip|ipv6} *<CLASS-NAME>*	Specifies the class where you want to resequence class entries.

Parameter	Description
<STARTING-SEQUENCE-NUMBER>	Specifies the sequence number to start resequencing from.
<INCREMENT>	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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
-------------------------------------------------------------------------------
IPv4       MY_IP_CLASS
         1 match                           igmp
           any
           any
        11 ignore                          udp
           any
           any
        21 match                           tcp
           192.168.0.1
           192.168.0.2
```

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                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
-------------------------------------------------------------------------------
IPv6       MY_IPV6_CLASS
         1 match                           any
           any
           1020::
         2 ignore                          udp
           any
           any
```

For more information on features that use this command, refer to the ACLs and Classifiers Policy 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>} 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>}`	Specifies either **all** classes be reset or specifies the type (**ip** for IPv4, or **ipv6** for IPv6) 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 Classifiers Policy 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

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.
`global`	Selects the globally applied policy.

Examples

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 Classifiers Policy 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} <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 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}` *<CLASS-NAME>*	Specifies a type of class, **ip** for IPv4, **ipv6** for IPv6.
<REMARK-ACTIONS>	Remark actions can be any of the following options: {**cos <*COS-VALUE*> | ip-precedence <IP-PRECEDENCE_ VALUE> | dscp <*DSCP-VALUE*>**} where:
`cos` *<COS-VALUE>*	Specifies the Class of Service (CoS) value.
`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

Parameter	Description
	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)
<POLICE-ACTIONS>	Police actions can be the following **{cir *<RATE-BPS>* exceed}** where:
`cir kbps` *<RATE-KBPS>*	Specifies a Committed Information Rate value in Kilobits per second. 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)# do 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)# do show policy
           Name
  Sequence Comment
           Class Type
                    action
-------------------------------------------------------------------------------
           MY_POLICY
        10
           MY_CLASS1 ipv6
                    drop
                    dscp AF21

        20 MY_TEST_POLICY
           MY_CLASS3 ipv4
                    mirror 1
```

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)# do show policy
           Name
  Sequence Comment
           Class Type
                    action
-------------------------------------------------------------------------------
           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)# do 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)# do show policy
           Name
  Sequence Comment
           Class Type
                    action
-------------------------------------------------------------------------------
           MY_POLICY
        20
           MY_CLASS3 ipv4
                    mirror 1
```

Removing a policy:

```
switch(config)# no policy MY_POLICY
switch(config)# do show policy
           Name
  Sequence Comment
           Class Type
                    action
-------------------------------------------------------------------------------
           MY_POLICY2
         2
           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 Classifiers Policy Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config` The `policy` command takes you into the `config-policy` 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
`<POLICY-NAME>`	Specifies the policy to be copied.
`<DESTINATION-POLICY>`	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 Classifiers Policy 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 Classifiers Policy 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 Classifiers Policy 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] [<CLASS-NAME>] [commands] [configuration]
```

Description

Shows class configuration information.

All parameters are optional.

Parameter	Description
`[ip | ipv6]`	Selects the class type for the display: **ip** for IPv4, **ipv6** for IPv6.
<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.

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 Classifiers Policy 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]
```

Syntax that filters by policies applied to an interface or VLAN:

```
show policy [interface <IF-NAME> [in] | vlan <VLAN-ID> [in]]
            [commands] [configuration]
```

Syntax that filters by the named policy:

```
show policy <POLICY-NAME> [commands] [configuration]
```

Syntax that filters by the globally applied policy:

```
show policy global [commands] [configuration]
```

Syntax that shows statistical information in the form of hit counts:

```
show policy hitcounts <POLICY-NAME> [interface <IF-NAME> [in] |
                      vlan <VLAN-ID> [in]]
```

Syntax that shows statistical information in the form of hit counts for the globally applied policy:

```
show policy hitcounts global
```

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, the statistics will be aggregated. 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
`interface <IF-NAME>`	Specifies the interface name.
`vlan <VLAN-ID>`	Specifies the VLAN.
`vni<VNI-ID>`	Specifies the VNI.
`in`	Selects the inbound (ingress) traffic direction.
`<POLICY-NAME>`	Specifies the policy name.
`commands`	Causes the policy definition to be shown as the commands and parameters used to create it rather than in tabular form.
`configuration`	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.
`global`	Selects the globally applied policy.
`hitcounts`	Selects the policy hit counts (statistics).

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
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count
```

Showing policy hit counts (statistics) for a policy applied everywhere (with 1/1/4 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  [ 0
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count

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
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count

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
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count

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  [ 0
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count
...
```

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
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count
```

Showing policy hit counts (statistics) for a policy applied on VLANs:

```
switch# show policy hitcounts My_Policy vlan 10
Statistics for Policy My_Policy:

vlan 10,20-30 (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
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count
Statistics for Policy My_Policy:

vlan 10,20-30 (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
kbps conform ]
                   -  10 match tcp any any ack
                   0  20 match icmpv6 1000::10 any count
```

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

Command History

Release	Modification
10.08	Added **[per-interface]** 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.

client-insight enable

```
client-insight enable
no client-insight enable
```

Description

Enables the Client Insight feature on the device. Client Insight is disabled by default at the device level.

The `no` form of the command disables Client Insight.

Examples

Enabling the Client Insight feature:

```
switch(config)# client-insight enable
```

Disabling the Client Insight feature:

```
switch(config)# no client-insight enable
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

client-insight on-boarding event logs

```
client-insight
   event-log
   client-onboarding
```

Description

Enables generation of event logs that lists the onboarding status of each client. Onboarding event logs are disabled by default. For onboarding event logs to work, the Client Insight feature should be enabled before client onboarding. Use the no form of the command to disable onboarding event logs for clients.

Parameter	Description
`event-log`	Configure client onboarding event logs.
`client-onboarding`	Enable client onboarding event logs.

Examples

Enabling client onboarding event logs:

```
switch(config)# client-insight event-log client-onboarding
```

Disabling client onboarding event logs:

```
switch(config)# no client-insight event-log client-onboarding
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

diag-dump client-insight basic

`diag-dump client-insight basic`

Description

Displays the status of the Client Insight feature—whether enabled or disabled globally. It also displays latencies for all active clients that are onboarded.

Examples

```
switch# diag-dump client-in basic
================================================================================
[Start] Feature client-insight Time : Tue Jul 25 05:32:14 2023
```

```
================================================================================
--------------------------------------------------------------------------------
[Start] Daemon client-insightd
--------------------------------------------------------------------------------

Global client-insight         = ENABLED
Client on-boarding event logs = ENABLED
Client dns on-boarding latency= ENABLED

Displaying client entries with (mac) as key.
Total number of entries: 2

MAC : 00:50:56:96:0e:3f
-----------------------
Overall on-boarding status         : successful
Overall on-boarding failure reason : -

L2 on-boarding detail
---------------------
L2 on-boarding status         : successful
L2 on-boarding failure reason : -
L2 on-boarding start time     : 07/25/2023 05:28:50.495425 UTC
L2 on-boarding end time       : 07/25/2023 05:28:50.495425 UTC
L2 on-boarding latency        : 0 min, 0 sec, 0 us
802.1x RADIUS latency         : -
MAC-Auth RADIUS latency       : -

L3 on-boarding detail
---------------------
IP on-boarding status           : successful
IP on-boarding failure reason   : -
L3 on-boarding latency          : 0 min, 3 sec, 455792 us

VLAN : 20
-----------
IP details
----------
IPv4 on-boarding status         : successful
IPv6 on-boarding status         : -

DHCPv4                                          DHCPv6
------                                          ------
Status         : successful                     Status         : -
Failure reason : -                              Failure reason : -
Start time     : 07/25/2023 05:28:50.485325 UTC Start time     : -
End time       : 07/25/2023 05:28:53.941117 UTC End time       : -

DNS details
-----------
DNS on-boarding status : successful
Failure reason         : -

Server IP: 11.11.11.2
---------------------
On-boarding latency  : 0 min, 0 sec, 306 us
DNS request time     : 07/25/2023 05:28:59.656937 UTC
DNS response time    : 07/25/2023 05:28:59.657243 UTC

Average latency:
Server IP: 11.11.11.2
---------------------
Average latency                       : 7091960 usec
```

```
DNS start time for latency calculation : 07/25/2023 05:23:51.335296 UTC
DNS end time for latency calculation   : 07/25/2023 05:28:51.323025 UTC
Number of DNS requests                 : 14

Server IP: 12.12.12.2
---------------------
Average latency                        : 7954 usec
DNS start time for latency calculation : 07/25/2023 05:23:51.335296 UTC
DNS end time for latency calculation   : 07/25/2023 05:28:51.323025 UTC
Number of DNS requests                 : 12

Server IP: 13.13.13.2
---------------------
Average latency                        : 7388 usec
DNS start time for latency calculation : 07/25/2023 05:23:51.335296 UTC
DNS end time for latency calculation   : 07/25/2023 05:28:51.323025 UTC
Number of DNS requests                 : 12
------------------------------------------------------------------------
[End] Daemon client-insightd
------------------------------------------------------------------------
========================================================================
[End] Feature client-insight
========================================================================
Diagnostic-dump captured for feature client-insight
```

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
6000 6100	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show capacities client-insight-client-limit

`show capacities client-insight-client-limit`

Description

Displays the maximum number of clients supported by the Client Insight feature on the switch.

Examples

```
switch# show capacities client-insight-client-limit

System Capacities: Filter Client-Insight client limit
```

```
Capacities Name                                                          Value
-------------------------------------------------------------------------------
Maximum number of clients supported by Client-Insight feature             4096
```

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
6000 6100	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show capacities-status client-insight-client-limit

```
show capacities-status client-insight-client-limit
```

Description

Displays the maximum number of clients learnt by the Client Insight feature on the switch.

Examples

```
switch# show capacities-status client-insight-client-limit
System Capacities Status: Filter Client-Insight client limit
Capacities Status Name                                    Value Maximum
-------------------------------------------------------------
Number of clients learnt by Client-Insight feature            0    4096
```

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
6000 6100	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show events -c client-insight

```
show events -c client-insight
```

Description

Displays all the events logged by the Client Insight feature.

Following events are logged by the Client Insight feature:

Table 1: *Events Logged by Client Insight*

Process	Event ID	Severity	Message	Description
client-insightd	14301	Info	`Client {mac} {vlans} on {port_name} successfully on-boarded. Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}`	Client successfully on-boarded with given timestamp values.
client-insightd	14302	Info	`Client {mac} {vlans} on {port_name} partial success in on-boarding. L2 status: {l2_ob_state} L3 status: {l3_ob_state}. Client on-boarding started at {ob_start_ts};L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}`	Client on-boarding is partial-successful with given timestamp values.
client-insightd	14303	Info	`Client {mac} on {port_name} failed to on-board with status: {onboarding_status} reason_code: {failure_phase_id}`	Client failed to on-board with given status and reason code.
client-insightd	14304	Info	`Maximum system wide client limit {client-number} reached`	Maximum system wide client limit is reached
client-insightd	14305	Info	`Maximum system wide client`	Maxiumum system wide client limit is reached

Process	Event ID	Severity	Message	Description
			`limit {client-number} reached`	
client-insightd	14306	Info	`Client {mac} successfully on-boarded on VLAN {vlans}; Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}; ARP to GW response received at {arp_end_ts}; DNS on-boarding to (dns_server_ip) completed at {dns_end_ts}`	Client successfully on-boarded with given timestamp values.
client-insightd	14307	Info	`Client {mac} on-boarded on VLANs {vlans} and failed on VLANs {failed_vlans}; Client on-boarding started at {ob_start_ts}; L2 complete at {l2_end_ts}; L3 complete at {l3_end_ts}; ARP to GW response received at {arp_end_ts}; DNS on-boarding to (dns_server_ip) completed at {dns_end_ts}; L2 status {l2_ob_state} failure_reason_code - {l2_failure_reason}; L3 status {l3_ob_state} failure_reason_code - {l3_failure_reason}; DNS on-boarding status {dns_status} failure_reason_code - {dns_failure_reason}`	Client on-boarding is partial-successful with given timestamp values.
client-insightd	14308	Info	`Client {mac} failed to on-board with status: {onboarding_status} in failure phase: {failure_phase_id} with reason: {failure_reason}`	Client failed to on-board with given status, phase_id and reason code.

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
6000 6100	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show tech client-insight

```
show tech client-insight
```

Description

Displays if the global Client Insight and client on-boarding event log features are enabled or disabled. Also displays the latencies for all active clients that are onboarded.

Examples

```
switch# show tech client-insight

=====================================================
Show Tech executed on Thu May 18 15:05:43 2022
=====================================================
=====================================================
[Begin] Feature client-insight
=====================================================
*********************************
Command : show client-insight
*********************************
Client Insight Information:
Global client-insight         = ENABLED
Client on-boarding event logs = ENABLED
=====================================================
[End] Feature client-insight
=====================================================
=====================================================
Show Tech commands executed successfully
=====================================================
```

Displaying L2, L3 client latencies and details:

```
switch# show tech client-insight
=====================================================
Show Tech executed on Thu Sep 22 06:34:16 2022
=====================================================
```

```
=====================================================
[Begin] Feature client-insight
=====================================================


*******************************
Command : diag-dump client-insight basic
*******************************
================================================================================
[Start] Feature client-insight Time : Thu Sep 22 06:34:16 2022
================================================================================
--------------------------------------------------------------------------------
[Start] Daemon client-insightd
--------------------------------------------------------------------------------

    Global client-insight         = ENABLED
    Client on-boarding event logs = ENABLED

  Displaying client entries with (mac) as key.
  Total number of entries: 1

MAC : 00:11:01:00:00:08
-----------------------
  Overall on-boarding status         : -
  Overall on-boarding failure reason : -

  L2 on-boarding detail
  ---------------------
    L2 on-boarding status         : successful
    L2 on-boarding failure reason : -
    L2 authentication start time  : 05/18/22 15:01:01.456789 UTC
    L2 authentication end time    : 05/18/22 15:01:02.123456 UTC
    L2 authentication latency     : 0 min, 0 sec, 666667 us
    802.1x RADIUS latency         : -
    MAC-Auth RADIUS latency       : 0 min, 0 sec, 332456 us

  L3 on-boarding detail
  ---------------------
    L3 on-boarding status           : in_progress
    L3 on-boarding failure reason   : -
    L3 on-boarding latency          : -

    VLAN : 10
    -----------
      IP details
      ----------
        IPv4 on-boarding status         : successful
        IPv6 on-boarding status         : -

        DHCPv4                                              DHCPv6
        ------                                              ------
          Status         : successful                       Status         : -
          Failure reason : -                                Failure reason : -
          Start time     : 05/18/22 15:01:02.456789 UTC     Start time     : -
          End time       : 05/18/22 15:01:02.999988 UTC     End time       : -

    VLAN : 20
    -----------
      IP details
      ----------
        IPv4 on-boarding status         : In_Progress
        IPv6 on-boarding status         : -
```

```
       DHCPv4                                              DHCPv6
       ------                                              ------
         Status         : In_Progress                       Status         : -
         Failure reason : -                                 Failure reason : -
         Start time     : 05/18/22 15:01:03.256485 UTC      Start time     : -
         End time       : -                                 End time       : -

  DNS details
  -----------
    Server IP: 172.16.1.8
    ---------------------
      Average latency                          : 0 min, 0 sec, 432456 us
      DNS start time for latency calculation   : 05/18/22 15:01:03.123456 UTC
      DNS end time for latency calculation     : 05/18/22 15:01:03.425466 UTC
      Number of DNS requests                   : 16

   Server IP: 2003::1
   ---------------------
      Average latency                          : 0 min, 0 sec, 432456 us
      DNS start time for latency calculation   : 05/18/22 15:01:03.123456 UTC
      DNS end time for latency calculation     : 05/18/22 15:01:03.425466 UTC
      Number of DNS requests                   : 16



-------------------------------------------------------------------------------
[End] Daemon client-insightd
-------------------------------------------------------------------------------
===============================================================================
[End] Feature client-insight
===============================================================================
Diagnostic-dump captured for feature client-insight
=====================================================
[End] Feature client-insight
=====================================================


=====================================================
Show Tech commands executed successfully
=====================================================
Show Tech took 43 seconds for execution

=====================================================
Show Tech executed on Thu Sep 22 06:34:16 2022
=====================================================
=====================================================
[Begin] Feature client-insight
=====================================================


*********************************
Command : diag-dump client-insight basic
*********************************
===============================================================================
[Start] Feature client-insight Time : Thu Sep 22 06:34:16 2022
===============================================================================
-------------------------------------------------------------------------------
[Start] Daemon client-insightd
-------------------------------------------------------------------------------
```

```
    Global client-insight         = ENABLED
    Client on-boarding event logs = ENABLED

  Displaying client entries with (mac) as key.
  Total number of entries: 1

MAC : 00:11:01:00:00:08
-----------------------
  Overall on-boarding status         : -
  Overall on-boarding failure reason : -

  L2 on-boarding detail
  ---------------------
    L2 on-boarding status         : successful
    L2 on-boarding failure reason : -
    L2 authentication start time  : 05/18/22 15:01:01.456789 UTC
    L2 authentication end time    : 05/18/22 15:01:02.123456 UTC
    L2 authentication latency     : 0 min, 0 sec, 666667 us
    802.1x RADIUS latency         : -
    MAC-Auth RADIUS latency       : 0 min, 0 sec, 332456 us

  L3 on-boarding detail
  ---------------------
    L3 on-boarding status           : in_progress
    L3 on-boarding failure reason   : -
    L3 on-boarding latency          : -

    VLAN : 10
    -----------
      IP details
      ----------
        IPv4 on-boarding status         : successful
        IPv6 on-boarding status         : -

        DHCPv4                                          DHCPv6
        ------                                          ------
          Status         : successful                     Status         : -
          Failure reason : -                              Failure reason : -
          Start time     : 05/18/22 15:01:02.456789 UTC   Start time     : -
          End time       : 05/18/22 15:01:02.999988 UTC   End time       : -

    VLAN : 20
    -----------
      IP details
      ----------
        IPv4 on-boarding status         : In_Progress
        IPv6 on-boarding status         : -

        DHCPv4                                          DHCPv6
        ------                                          ------
          Status         : In_Progress                    Status         : -
          Failure reason : -                              Failure reason : -
          Start time     : 05/18/22 15:01:03.256485 UTC   Start time     : -
          End time       : -                              End time       : -

  DNS details
  -----------
    Server IP: 172.16.1.8
    ---------------------
      Average latency                       : 0 min, 0 sec, 432456 us
      DNS start time for latency calculation : 05/18/22 15:01:03.123456 UTC
      DNS end time for latency calculation   : 05/18/22 15:01:03.425466 UTC
```

```
      Number of DNS requests                 : 16

   Server IP: 2003::1
   --------------------
      Average latency                        : 0 min, 0 sec, 432456 us
      DNS start time for latency calculation : 05/18/22 15:01:03.123456 UTC
      DNS end time for latency calculation   : 05/18/22 15:01:03.425466 UTC
      Number of DNS requests                 : 16



-------------------------------------------------------------------------
[End] Daemon client-insightd
-------------------------------------------------------------------------
=========================================================================
[End] Feature client-insight
=========================================================================
Diagnostic-dump captured for feature client-insight
=====================================================
[End] Feature client-insight
=====================================================


=====================================================
Show Tech commands executed successfully
=====================================================
Show Tech took 43 seconds for execution
```

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
6000 6100	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

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 alias command should not be configured for CLI commands that contain sensitive information.

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 **$1** through $*n*, 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 `config` or `config-vlan-10`	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.

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. 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 **show history** 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. If the **id** parameter is not specified, the **repeat** 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
```

Description

Shows the configured session timeout value.

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
```

Description

Shows the command aliases that are defined on the switch.

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. By default, the output of this command will display up to 500 commands previously executed by the user in the current session.

This command will not display any commands entered by the user that contain sensitive information such as plain text passwords or keys. The output will only be valid for the current boot and not for commands executed in the previous boot.

Parameter	Description
`all-sessions`	Specifies that the output includes commands from the current session as well as previous sessions logged out of by the user.

Parameter	Description
	When you include the **all-sessions** parameter, the output of this command will display up to 1000 commands previously executed by the user.
`timestamp`	Specifies that the output include the time of execution of each command in the command history.

If you include 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
5     configure
4     session-timeout 0
3     exit
2     show feature-pack
1     show logging
```

Showing a list of commands executed during the current CLI session, with timestamps:

```
switch# show history timestamp
5     Mon May  6 18:42:05 2024        configure
4     Mon May  6 18:42:08 2024        session-timeout 0
3     Mon May  6 18:42:10 2024        exit
2     Mon May  6 18:42:19 2024        show feature-pack
1     Mon May  6 18:42:29 2024        show logging
```

Showing a list of commands executed by the user both in the current session and during all previous CLI sessions:

```
switch# show history all-sessions
12    configure
11    session-timeout 0
10    exit
9     show feature-pack
8     show logging
7     configure
6     exit
5     configure
4     alias abcd show running-config
3     abcd
2     show tech
1     exit
```

Showing a list of commands executed by the user both in the current session and during all previous sessions, with timestamps:

```
switch# show history all-sessions timestamp
12     Mon May  6 18:42:05 2024        configure
11     Mon May  6 18:42:08 2024        session-timeout 0
10     Mon May  6 18:42:10 2024        exit
9      Mon May  6 18:42:19 2024        show feature-pack
8      Mon May  6 18:42:29 2024        show logging
7      Mon May  6 18:42:44 2024        configure
6      Mon May  6 18:42:55 2024        exit
5      Mon May  6 18:45:41 2024        configure
4      Mon May  6 18:45:55 2024        alias abcd show running-config
3      Mon May  6 18:45:59 2024        abcd
2      Mon May  6 18:46:09 2024        show tech
1      Mon May  6 18:46:14 2024        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	The **all-sessions** 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.

Chapter 16
CLI user session management commands

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: **YYYY-MM-DD**.

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: **YYYY-MM-DD**.

Parameter	Description
<TIME>	Specifies the time in 24-hour clock format. Seconds are optional. Format: **HH:MM** or **HH:MM:SS**.

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: **HH:MM** or **HH:MM:SS**.

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 https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

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 **no** 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.

Classes of traffic

The different classes of traffic that can be individually configured are:

- `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.
- `dhcp`: Dynamic Host Configuration Protocol packets. Also includes snooped DHCP packets if DHCP snooping is enabled.
- `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-security-ipv6`: IPv6 Internet Control Message Protocol packets intercepted and inspected.
- `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.
- `igmp`: Internet Group Management Protocol packets.
- `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.
- `manageability`: Unicast IP packets addressed to the switch for specific protocols that do not have a dedicated CoPP class like HTTP, SSH, Telnet, and RADIUS.
- `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.
- `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.
- `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.
- `unresolved-ip-unicast`: Packets to be software forwarded by the management processor.

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
<NAME>	Specifies the name of the policy to apply. Length: 1 to 64 characters.
`default`	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>}
no class <CLASS> {drop | priority <PRIORITY> rate <RATE>}
```

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 the configuration for the class. Traffic for the class will be prioritized and regulated using the factory default configuration for the class. Use the **show copp-policy factory-default** command to display the factory default CoPP policy. 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.
`drop`	Drop packets matching the selected class.
`priority` *<PRIORITY>*	Specifies the priority for packets matching the selected class. Range: 0 to 6.
`rate` *<RATE>*	Specifies the maximum rate, in packets per second (pps), for packets matching the selected class. Range: 25 to 99999.

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.

```
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:

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>`

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: 25 to 99999.

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 hardware rate pps
--------------------- ---- -------- -------- -----------------
igmp                       6        5000     5000
lacp                       2        2000     2000
default                    1        6000     6000
switch# config terminal
switch(config)# copp-policy My_CoppPolicy
switch(config-copp)# class stp priority 4 rate 4000
switch(config-copp)# do show copp-policy My_CoppPolicy
class                 drop priority rate pps hardware rate pps
--------------------- ---- -------- -------- -----------------
igmp                       6        5000     5000
lacp                       2        2000     2000
default                    1        6000     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 applied
--------------------- ---- -------- -------- -------
igmp                       6        5000     yes
lacp                       2        2000     yes
stp                        4        4000     no
default                    1        6000     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 hardware rate pps
--------------------- ---- -------- -------- -----------------
igmp                       6        5000     5000
lacp                       2        2000     2000
default                    1        6000     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]`

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 **not** the active settings.

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:

Displaying the `default` policy:

```
switch# show copp-policy default
class                drop priority rate pps hardware rate pps
-------------------- ---- -------- -------- -----------------
arp-broadcast              2        1250     1250
arp-unicast                3        825      825
    <--OUTPUT OMITTED FOR BREVITY-->
default                    2        4225     4225
```

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]
```

Description

Display the configuration for the factory-default CoPP policy.

Parameter	Description
`commands`	Displays output as CLI commands.

Example

Displaying the factory-default policy:

```
switch# show copp-policy factory-default
class                drop priority rate pps
-------------------- ---- -------- --------
arp-broadcast              2        1250
arp-unicast                3        825
    <--OUTPUT OMITTED FOR BREVITY-->
default                    2        4225
```

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 hardware rate pps
--------------------- ---- -------- -------- -----------------
igmp                        6        5000     5000
lacp                        2        2000     2000
default                     1        6000     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
    class lacp priority 2 rate 2000
    default-class priority 1 rate 6000
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 applied
--------------------- ---- -------- -------- -------
igmp                        6        5000     yes
lacp                        2        2000     yes
default                     1        6000     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
    class lacp priority 2 rate 2000
    default-class priority 1 rate 6000
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]
```

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 **class** for which to display statistics.
default-class	Displays statistics for the default class.
non-zero	Displays statistics for all classes with non-zero statistics.

Usage

If a single class is specified, the priority and rate that has been programmed in hardware for that class will be shown.

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:
    packets passed   : 1000              packets dropped  : 1500
Class: default
    packets passed   : 400               packets dropped  : 600
Class: arp-broadcast
    packets passed   : 500               packets dropped  : 800
        <--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             : 2
    rate (pps)           : 4225


    packets passed   : 400               packets dropped  : 600
```

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             : 2
    rate (pps)           : 1250

    packets passed   : 500               packets dropped  : 800
```

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 **debug** 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 **debug *<MODULE-NAME>*** 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 **debug**. Optional.
`emer`	Specifies storage of debug logs with a severity level of **emergency** only.
`crit`	Specifies storage of debug logs with severity level of **critical** and above.
`alert`	Specifies storage of debug logs with severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Specifies storage of debug logs with severity level of **warning** and above.
`info`	Specifies storage of debug logs with severity level of **info** and above.

Parameter	Description
`debug`	Specifies storage of debug logs with severity level of **debug** (default).
`port`	Displays debug logs for the specified port, for example **1/1/1**.
`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 **A:B:C:D:E:F**.
`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
`all`	Enables all submodules for the db log.
`sub-module`	Enables debug logging for supported submodules. Specify **rx** or **tx** debug logs.
`filter`	Specifies supported filters for the db log. Specify **table**, **column**, or **client**. Optional
`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 **debug**. Optional.
`emer`	Specifies storage of debug logs with a severity level of **emergency** only.
`crit`	Specifies storage of debug logs with severity level of **critical** and above.
`alert`	Specifies storage of debug logs with severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Specifies storage of debug logs with severity level of **warning** and above.
`info`	Specifies storage of debug logs with severity level of **info** and above.
`debug`	Specifies storage of debug logs with severity level of **debug** (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 **syslog**.
`file`	Specifies that debug logs are stored in **file**.
`console`	Specifies that debug logs are stored in **console**.
`buffer`	Specifies that debug logs are stored in **buffer** (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**debug**. Optional.
`emer`	Specifies storage of debug logs with a severity level of **emergency** only.
`crit`	Specifies storage of debug logs with severity level of **critical** and above.
`alert`	Specifies storage of debug logs with severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Specifies storage of debug logs with severity level of **warning** and above.
`info`	Specifies storage of debug logs with severity level of **info** and above.
`debug`	Specifies storage of debug logs with severity level of **debug** (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.

show debug

```
show debug
```

Description

Displays the enabled debug types.

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
default
```

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**debug**. Optional.
`emer`	Displays debug logs with a severity level of **emergency** only.
`crit`	Displays debug logs with a severity level of **critical** and above.
`alert`	Displays debug logs with a severity level of **alert** and above.
`err`	Specifies storage of debug logs with severity level of **error** and above.
`notice`	Specifies storage of debug logs with severity level of **notice** and above.
`warning`	Displays debug logs with a severity level of **warning** and above.
`info`	Displays debug logs with a severity level of **info** and above.
`debug`	Displays debug logs with a severity level of **debug** (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
```

Description

Displays the configured debug destination and severity.

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.

aaa authentication port-access allow-cdp-auth

```
aaa authentication port-access allow-cdp-auth
no aaa authentication port-access allow-cdp-auth
```

Description

Use this command to allow or block authentication on the CDP (Cisco Discovery Protocol) BPDU (Bridge Protocol Data Unit) . This is allowed by default. The **no** form of this command prevents authentication on CDP packets received on the port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

Examples

Allowing authentication on a CDP CPDU on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-cdp-auth
```

Allowing authentication on a CDP CPDU on a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# aaa authentication port-access allow-cdp-auth
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access allow-cdp-bpdu

```
aaa authentication port-access allow-cdp-bpdu
no aaa authentication port-access allow-cdp-bpdu
```

Description

Allows all packets related to the CDP (Cisco Discovery Protocol) BPDU (Bridge Protocol Data Unit) on a secure port or LAG. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts. The **no** form of this command blocks the CDP BPDU on a secure port. On a nonsecure port, the command has no effect.

Examples

Allowing a CDP BPDU on secure port **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-cdp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
!
vlan 1
aaa authentication port-access mac-auth
    enable
aaa authentication port-access dot1x authenticator
    enable
interface 1/1/1
    no shutdown
    vlan access 1
    aaa authentication port-access allow-cdp-bpdu
    aaa authentication port-access mac-auth
        enable
    aaa authentication port-access dot1x authenticator
    enable

switch(config-if)# do show port-access device-profile interface all
Port 1/1/1, Neighbor-Mac 00:0c:29:9e:d1:20
    Profile Name    : access_switches
    LLDP Group      :
    CDP Group       : aruba-ap_cdp
    Role            : test_ap_role
    Status          : In Progress
    Failure Reason  :
```

Blocking LLDP packet on secure port **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access allow-cdp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
!
```

```
vlan 1
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown
    vlan access 1
    aaa authentication port-access mac-auth
        enable
```

Allowing a CDP BPDU on LAG **1**:

```
switch(config)# interface lag 1
switch(config-lag-if)# aaa authentication port-access allow-cdp-bpdu
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access allow-cdp-proxy-logoff

```
aaa authentication port-access allow-cdp-proxy-logoff
no aaa authentication port-access allow-cdp-proxy-logoff
```

Description

Allows a client to be logged off from the system via a special TLV in the CDP packet. By default, proxy logoff via CDP packet support is disabled. When **allow-cdp-proxy-logoff** is enabled, TLV received from CDP packets corresponding to logoff processing will be read and logoff is issued to the clients. This only works on client authentication enabled ports and **aaa authentication port-access allow-cdp-bpdu** must be enabled to process. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

Examples

Allowing a client to be logged off from the system via a special TLV in the CDP packet:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-cdp-proxy-logoff
switch(config-if)# show running-config interface 1/1/1
interface 1/1/1
    no shutdown

    vlan access 1
    aaa authentication port-access allow-cdp-bpdu
    aaa authentication port-access allow-cdp-proxy-logoff
    aaa authentication port-access allow client-limit 2
    aaa authentication port-access dot1x authenticator
        enable
    aaa authentication port-accss mac-auth
        enable
    exit
```

The aaa authentication port-access allow-cdp-proxy-logoff command can also be issued from a LAG port context

```
switch(config)# interface lag 1
switch(config-lag if)# aaa authentication port-access allow-cdp-proxy-logoff
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config-if config-lag-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access allow-lldp-bpdu

```
aaa authentication port-access allow-lldp-bpdu
no aaa authentication port-access allow-lldp-bpdu
```

Description

Allows all packets related to the LLDP BPDU (Bridge Protocol Data Unit) on a secure port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

The **no** form of this command blocks the LLDP BPDU on a secure port. On a nonsecure port, the command has no effect.

Examples

Allowing an LLDP BPDU on secure port **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-lldp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
!
vlan 1
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown

    vlan access 1
    aaa authentication port-access allow-lldp-bpdu
    aaa authentication port-access mac-auth
        enable

switch(config-if)# do show port-access device-profile interface all
Port 1/1/1, Neighbor-Mac 00:0c:29:9e:d1:20
    Profile Name    : access_switches
    LLDP Group      : 2920-grp
    CDP Group       :
    Role            : local_2920_role
    Status          : Profile Applied
    Failure Reason  :
```

Blocking LLDP BPDU on secure port **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access allow-lldp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000led locator on
!
!
vlan 1
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown

    vlan access 1
    aaa authentication port-access mac-auth
    enable
```

Allowing an LLDP BPDU on a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)#aaa authentication port-access allow-lldp-bpdu
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

associate cdp-group

```
associate cdp-group <GROUP-NAME>
no associate cdp-group <GROUP-NAME>
```

Description

Associates a CDP (Cisco Discovery Protocol) group with a device profile. A maximum of two CDP groups can be associated with a device profile.

The **no** form of this command removes a CDP group from a device profile.

Parameter	Description
<GROUP-NAME>	Specifies the name of the CDP group to associate with this device profile. Range: 1 to 32 alphanumeric characters.

Examples

Associating the CDP group **my-cdp-group** with the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate cdp-group my-cdp-group
```

Removing the CDP group **my-cdp-group** from the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate cdp-group my-cdp-group
```

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
6000 6100	`config-device-profile`	Administrators or local user group members with execution rights for this command.

associate lldp-group

```
associate lldp-group <GROUP-NAME>
no associate lldp-group <GROUP-NAME>
```

Description

Associates an LLDP group with a device profile. A maximum of two LLDP groups can be associated with a device profile

The **no** form of this command removes an LLDP group from a device profile.

Parameter	Description
<GROUP-NAME>	Specifies the name of the LLDP group to associate with the device profile. Range: 1 to 32 alphanumeric characters.

Examples

Associating the LLDP group **my-lldp-group** with the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate lldp-group my-lldp-group
```

Removing the LLDP group **my-lldp-group** from the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate lldp-group my-lldp-group
```

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
6000 6100	`config-device-profile`	Administrators or local user group members with execution rights for this command.

associate mac-group

```
associate mac-group <GROUP-NAME>
no associate mac-group <GROUP-NAME>
```

Description

Associates a MAC group with a device profile. A maximum of two MAC groups can be associated with a device profile.

The **no** form of this command removes a MAC group from a device profile.

Parameter	Description
<GROUP-NAME>	Specifies the name of the MAC group to associate with this device profile. Range: 1 to 32 alphanumeric characters.

Examples

Associating the MAC group **mac01-group** with the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate mac-group mac01-group
```

Removing the MAC group **mac01-group** from the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate mac-group mac01-group
```

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
6000 6100	`config-device-profile`	Administrators or local user group members with execution rights for this command.

associate role

```
associate role <ROLE-NAME>
no associate role <ROLE-NAME>
```

Description

Associates a role with a device profile. Only one role can be associated with a device profile. For information on how to configure a role, see the port access role information in the *Security Guide*.

The **no** form of this command removes a role from a device profile.

Parameter	Description
<ROLE-NAME>	Specifies the name of the role to associate with the device profile. Range: 1 to 64 alphanumeric characters.

Examples

Associating the role **my-role** with the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# associate role my-role
```

Removing the role **my-role** from the device profile **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no associate role my-role
```

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
6000 6100	`config-device-profile`	Administrators or local user group members with execution rights for this command.

disable

```
disable
no disable
```

Description

Disables a device profile.

The **no** form of this command enables a device profile.

Examples

Disabling a device profile:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# disable
```

Enabling a device profile named profile01:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no 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
6000 6100	`config-device-profile`	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables a device profile.

The **no** form of this command disables a device profile.

Examples

Enabling a device profile:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# enable
```

Disabling a device profile named profile01:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)# no enable
```

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	config-device-profile	Administrators or local user group members with execution rights for this command.

ignore (for CDP groups)

```
ignore [seq <SEQ-NUM>] {platform <PLATFORM> | sw-version <SWVERSION> |
     voice-vlan-query <VLAN-ID>}
no ignore [seq <SEQ-ID>] {platform <PLATFORM> | sw-version <SWVERSION> |
     voice-vlan-query <VLAN-ID>}
```

Description

Defines a rule to ignore devices for a CDP (Cisco Discovery Protocol) group. Up to 64 match/ignore rules can be defined for a group.

The **no** form of this command removes a rule for ignoring devices from a CDP group.

Parameter	Description
seq *<SEQ-ID>*	Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.
platform *<PLATFORM>*	Specifies the hardware or model details of the neighbor. Range: 1 to 128 alphanumeric characters.
sw-version *<SWVERSION>*	Specifies the software version of the neighbor. Range: 1 to 128 alphanumeric characters.
voice-vlan-query *<VLAN-ID>*	Specifies the VLAN query value of the neighbor. Range: 1 to 65535.

Examples

Adding a rule to the CDP group **grp01** that ignores a device that transmits **PLATFORM01** in the platform TLV:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# ignore platform PLATFORM01
```

Adding a rule to the CDP group **grp01** that ignores a device that transmits **SWVERSION** in software version TLV:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# ignore sw-version SWVERSION
```

Removing the rule that matches the sequence number **25** from the CDP group named **grp01**.

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# no ignore seq 25
```

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
6000 6100	config-cdp-group	Administrators or local user group members with execution rights for this command.

ignore (for LLDP groups)

```
ignore [seq <SEQ-ID>] {sys-desc <SYS-DESC> | sysname <SYS-NAME> |
     vendor-oui <VENDOR-OUI> [type <KEY> [value <VALUE>]]}
no ignore [seq <SEQ-ID>] {sys-desc <SYS-DESC> | sysname <SYS-NAME> |
     vendor-oui <VENDOR-OUI> [type <KEY> [value <VALUE>]]}
```

Description

Defines a rule to ignore devices for an LLDP group. Up to 64 match/ignore rules can be defined for a group.

The **no** form of this command removes a rule for ignoring devices from an LLDP group.

Parameter	Description
seq *<SEQ-ID>*	Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one

Parameter	Description
	rule matches the command entered, the rule with the lowest ID takes precedence.
`sys-desc <SYS-DESC>`	Specifies the LLDP system description type-length-value (TLV). Range: 1 to 256 alphanumeric characters.
sysname <SYS-NAME>	Specifies the LLDP system name TLV. Range: 1 to 64 alphanumeric characters.
`vendor-oui <VENDOR-OUI>`	Specifies the LLDP system vendor OUI TLV. Range: 1 to 6 alphanumeric characters.
`type <KEY>`	Specifies the vendor OUI subtype key. Optional.
`value <VALUE>`	Specifies the vendor OUI subtype value. Range: 1 to 256 alphanumeric characters.

Examples

Adding a rule to the LLDP group **grp01** that ignores a device that transmits **PLATFORM01** in the system description TLV:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# ignore sys-desc PLATFORM01
```

Removing the rule that matches the sequence number **25** from the LLDP group named **grp01**.

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# no match seq 25
```

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
6000 6100	`config-lldp-group`	Administrators or local user group members with execution rights for this command.

ignore (for MAC groups)

`[seq <SEQ-ID>] ignore {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}`
`no [seq <SEQ-ID>] ignore {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}`

Description

Defines a rule to ignore devices for a MAC group based on the criteria of MAC address, MAC address mask, or MAC Organizational Unique Identifier (OUI). Up to 64 ignore rules can be defined for a group.

The **no** form of this command removes a rule for ignoring devices from a MAC group.

Parameter	Description
`seq <SEQ-ID>`	Specifies the entry sequence ID of the rule to create or modify a MAC group. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence. Range: **1** to **4294967295**.
`mac <MAC-ADDR>`	Specifies the MAC address of the device to ignore.
`mac-mask <MAC-MASK>`	Specifies the MAC address mask to ignore devices in that range. Supported MAC address masks: **/32** and **/40**.
`mac-oui <MAC-OUI>`	Specifies the MAC OUI to ignore devices in that range. Supports MAC OUI address of maximum length of 24 bits.

Usage

To achieve the required configuration of matches for devices, it is recommended to first ignore the devices that you do not want to add. Then match the criteria for the rest of the devices that you want to add to the MAC group.

For example, if you want to ignore a specific device but add all the other devices that belong to a MAC OUI, then you must first configure the ignore criteria with a lower sequence number. And then configure match criteria with a higher sequence number.

Examples

Adding a rule to the MAC group **grp01** to ignore a device based on MAC address, but match all other devices belonging to a MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac 1a:2b:3c:4d:5e:6f
switch(config-mac-group)# match mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
!
!
ssh server vrf
!
!
!
!
!
vlan 1
```

```
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
     seq 10 ignore mac 1a:2b:3c:4d:5e:6f
     seq 20 match mac-oui 1a:2b:3c

```
```

Adding a rule to the MAC group **grp01** to ignore devices based on MAC address mask, but match all other devices belonging to a MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac-mask 1a:2b:3c:4d/32
switch(config-mac-group)# match mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
!
!
ssh server vrf
!
!
!
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
     seq 10 ignore mac-mask 1a:2b:3c:4d/32
     seq 20 match mac-oui 1a:2b:3c

```
```

Adding a rule to the MAC group **grp01** that ignores a device based on complete MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac 1a:2b:3c:4d:5e:6f
```

Adding a rule to the MAC group **grp02** that ignores devices based on MAC mask:

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac-mask 1a:2b:3c:4d:5e/40
switch(config-mac-group)# ignore mac-mask 18:e3:ab:73/32
```

Adding a rule to the MAC group **grp03** that ignores devices based on MAC OUI:

```
switch(config)# mac-group grp03
switch(config-mac-group)# ignore mac-oui 81:cd:93
```

Adding a rule to the MAC group **grp01** that ignores devices with a sequence number and based on MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 ignore mac b2:c3:44:12:78:11
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
    seq 10 ignore mac b2:c3:44:12:78:11

```
```

Removing the rule from the MAC group **grp01** based on sequence number:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no ignore seq 10
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01

```
```

Adding a rule to the MAC group **grp01** that ignores devices with MAC entry sequence number and based on MAC OUI:

```
switch(config)# mac-group grp01
switch(config)#  mac-group grp01
switch(config-mac-group)# seq 10 ignore mac b2:c3:44:12:78:11
switch(config-mac-group)# seq 20 ignore mac-oui 1a:2b:3c
switch(config-mac-group)# seq 30 ignore mac-mask 71:14:89:42/32
switch(config-mac-group)# exit
switch(config)#
```

```
switch(config)# ^Z

switch#
switch#
switch# show running-config
Current configuration:
!
!Version AOS-CX PL.10.06.0002
!export-password: default
!
!
!
!
ssh server vrf default
vlan 1
spanning-tree
mac-group grp01
     seq 10 ignore mac b2:c3:44:12:78:11
     seq 20 ignore mac-oui 1a:2b:3c
     seq 30 ignore mac-mask 71:14:89:42/32
interface 1/1/1
    no shutdown
    vlan access 1
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
!
!
!
!
!
https-server vrf default
```

Removing the rule from the MAC group **grp01** based on sequence number and MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no seq 20 ignore mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
     seq 10 ignore mac b2:c3:44:12:78:11
     seq 30 ignore mac-mask 71:14:89:f3/32


```
```

Removing the rule that matches the sequence number **25** from the MAC group named **grp01**.

```
switch(config)# mac-group grp01
switch(config-mac-group)# no ignore seq 25
```

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
6000 6100	`config-mac-group`	Administrators or local user group members with execution rights for this command.

mac-group

```
mac-group <MAC-GROUP-NAME>
no mac-group <MAC-GROUP-NAME>
```

Description

Creates a MAC group or modifies an existing MAC group. A MAC group is used to classify connected devices based on the MAC address details, such as mask or OUI.

A maximum of 32 MAC groups can be configured on the switch. A maximum of 2 MAC groups can be associated with a device profile. Each group accepts 64 match or ignore commands.

The **no** form of this command removes a MAC group.

Parameter	Description
<MAC-GROUP-NAME>	Specifies the name of the MAC group to create or modify. The maximum number of characters supported is 32.

Examples

Creating a MAC group named **grp01**:

```
switch(config)# mac-group grp01
switch(config-mac-group)# exit
```

Removing a MAC group named **grp01**:

```
switch(config)# no mac-group grp01
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

match (for CDP groups)

```
match [seq <SEQ-ID>] {platform <PLATFORM> | sw-version <SWVERSION> |
     voice-vlan-query <VLAN-ID>}
no match [seq <SEQ-ID>] {platform <PLATFORM> | sw-version <SWVERSION> |
     voice-vlan-query <VLAN-ID>}
```

Description

Defines a rule to match devices for a CDP group. A maximum of 32 CDP groups can be configured on the switch. Up to 64 match or ignore rules can be defined for each group.

The **no** form of this command removes a rule for adding devices to a CDP group.

Parameter	Description
`seq <SEQ-ID>`	Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.
`platform <PLATFORM>`	Specifies the hardware or model details of the neighbor. Range: 1 to 128 alphanumeric characters.
`sw-version <SWVERSION>`	Specifies the software version of the neighbor. Range: 1 to 128 alphanumeric characters.
`voice-vlan-query <VLAN-ID>`	Specifies the VLAN query value of the neighbor. Range: 1 to 65535.

Examples

Adding rules to match a Cisco device with a specific software version on VLAN **512** to the CDP group **grp01**:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match platform CISCO
switch(config-cdp-group)# match sw-version 11.2(12)P
switch(config-cdp-group)# match voice-vlan-query 512
switch(config-cdp-group)# match seq 50 platform cisco sw-version 11.2(12)P voice-
vlan-query 512
switch(config-cdp-group)# exit
switch(config)# do show running-config

Current configuration:
!
!Version AOS-CX Virtual.10.0X.000
!export-password: default
led locator on
!
!
vlan 1
port-access cdp-group grp01
     seq 10 match platform CISCO
     seq 20 match sw-version 11.2(12)P
     seq 30 match voice-vlan-query 512
     seq 50 match platform cisco sw-version 11.2(12)P voice-vlan-query 512
```

Removing a rule that matches the sequence number **25** from the CDP group named **grp01**:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# no match seq 25
```

Adding a rule that matches the value of vendor-OUI **000b86** to the CDP group named **grp01**:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match vendor-oui 000b86
```

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
6000 6100	config-cdp-group	Administrators or local user group members with execution rights for this command.

match (for LLDP groups)

```
match [seq <SEQ-ID>] {sys-desc <SYS-DESC> | sysname <SYS-NAME> |
     vendor-oui <VENDOR-OUI> [type <KEY> [value <VALUE>]]}
no match [seq <SEQ-ID>] {sys-desc <SYS-DESC> | sysname <SYS-NAME> |
     vendor-oui <VENDOR-OUI> [type <KEY> [value <VALUE>]]}
```

Description

Defines a rule to match devices for an LLDP group. Up to 64 match/ignore rules can be defined for a group.

The **no** form of this command removes a rule.

Parameter	Description
seq *<SEQ-ID>*	Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.
sys-desc *<SYS-DESC>*	Specifies the LLDP system description type-length-value (TLV). Range: 1 to 256 alphanumeric characters.
sysname *<SYS-NAME>*	Specifies the LLDP system name TLV. Range: 1 to 64 alphanumeric characters.

Parameter	Description
`vendor-oui <VENDOR-OUI>`	Specifies the LLDP system vendor OUI TLV. Range: 1 to 6 alphanumeric characters.
`type <KEY>`	Specifies the vendor OUI subtype key.
`value <VALUE>`	Specifies the vendor OUI subtype value. Range: 1 to 256 alphanumeric characters.

Examples

Adding rules that match the LLDP system description **ArubaSwitch** and system name **Aruba** to the LLDP group named **grp01**:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# match sys-desc ArubaSwitch
switch(config-lldp-group)# match sysname Aruba
switch(config)# do show running-config

Current configuration:
!
!Version AOS-CX Virtual.10.0X.000
!export-password: default
led locator on
!
!
vlan 1
port-access lldp-group grp01
     seq 10 match sys-desc ArubaSwitch
     seq 20 match sysname Aruba
```

Removing a rule that matches the sequence number **25** from an LLDP group named **grp01**:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# no match seq 25
```

Adding a rule that matches the value of vendor-OUI **000b86** with type of **1** to the LLDP group named **grp01**:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# match vendor-oui 000b86 type 1
```

Adding a rule that matches the value of vendor-OUI **000c34** to the LLDP group named **grp01**:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)# match vendor-oui 000c34
```

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
6000 6100	`config-lldp-group`	Administrators or local user group members with execution rights for this command.

match (for MAC groups)

```
[seq <SEQ-ID>] match {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}
no [seq <SEQ-ID>] match {mac <MAC-ADDR> | mac-mask <MAC-MASK> | mac-oui <MAC-OUI>}
```

Description

Defines a rule to match devices for a MAC group based on the criteria of MAC address, MAC address mask, or MAC Organizational Unique Identifier (OUI). Up to 64 match rules can be defined for a group.

You must not configure the following special MAC addresses:

- Null MAC—For example, 00:00:00:00:00:00 or 00:00:00/32
- Multicast MAC
- Broadcast MAC—For example, ff:ff:ff:ff:ff:ff
- System MAC

Although the switch accepts these addresses, it will not process these addresses for the local MAC match feature.

The **no** form of this command removes a rule for adding devices to a MAC group.

The number of clients that can onboard based on the match criteria is configured in the **aaa authentication port-access client-limit** command. For information about this command, see the *Security Guide* for your switch.

Parameter	Description
`seq <SEQ-ID>`	Specifies the entry sequence ID of the rule to create or modify a MAC group. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence. Range: **1** to **4294967295**.
`mac <MAC-ADDR>`	Specifies the MAC address of the device.
`mac-mask <MAC-MASK>`	Specifies the MAC address mask to add devices in that range. Supported MAC address masks: **/32** and **/40**.
`mac-oui <MAC-OUI>`	Specifies the MAC OUI to add devices in that range. Supports MAC OUI address of maximum length of 24 bits.

Examples

Adding a device to the MAC group **grp01** based on complete MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# match mac 1a:2b:3c:4d:5e:6f
switch(config-mac-group)# exit
```

Adding devices to the MAC group **grp02** based on MAC mask:

```
switch(config)# mac-group grp01
switch(config-mac-group)# match mac-mask 1a:2b:3c:4d:5e/40
switch(config-mac-group)# match mac-mask 18:e3:ab:73/32
switch(config-mac-group)# exit
```

Adding devices to the MAC group **grp03** based on MAC OUI:

```
switch(config)# mac-group grp03
switch(config-mac-group)# match mac-oui 81:cd:93
switch(config-mac-group)# exit
```

Adding devices to the MAC group **grp01** with MAC entry sequence number and based on MAC address:

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 match mac b2:c3:44:12:78:11
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
    seq 10 match mac b2:c3:44:12:78:11

```
```

Removing devices from the MAC group **grp01** based on sequence number:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no match seq 10
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
```
```

```
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01

```

Adding devices to the MAC group **grp01** with MAC entry sequence number and based on MAC address, MAC address mask, and MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 match mac b2:c3:44:12:78:11
switch(config-mac-group)# seq 20 match mac-oui 1a:2b:3c
switch(config-mac-group)# seq 30 match mac-mask 71:14:89:f3/32
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
     seq 10 match mac b2:c3:44:12:78:11
     seq 20 match mac-oui 1a:2b:3c
     seq 30 match mac-mask 71:14:89:f3/32

```

Removing devices from the MAC group **grp01** based on MAC OUI:

```
switch(config)# mac-group grp01
switch(config-mac-group)# no seq 20 match mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp01
     seq 10 match mac b2:c3:44:12:78:11
     seq 30 match mac-mask 71:14:89:f3/32


```

Adding devices to the MAC group **grp03** with MAC entry sequence number and based on MAC address mask:

```
switch(config)# mac-group grp03
switch(config-mac-group)# seq 10 match mac-mask 10:14:a3:b7:55/40
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp03
     seq 10 match mac-mask 10:14:a3:b7:55/40

```

Removing devices from the MAC group **grp03** based on MAC address mask:

```
switch(config)# mac-group grp03
switch(config-mac-group)# no seq 10 match mac-mask 10:14:a3:b7:55/40
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface vlan 1
    no shutdown
    ip dhcp
mac-group grp03

```

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
6000 6100	config-mac-group	Administrators or local user group members with execution rights for this command.

port-access cdp-group

```
port-access cdp-group <CDP-GROUP-NAME>
no port-access cdp-group <CDP-GROUP-NAME>
```

Description

Creates a CDP (Cisco Discovery Protocol) group or modifies an existing CDP group. A CDP Group is used to classify connected devices based on the CDP packet details advertised by the device. A maximum of 32 CDP groups can be configured on the switch. Each group accepts 64 match/ignore commands.

The **no** form of this command removes a CDP group.

Parameter	Description
<CDP-GROUP-NAME>	Specifies the name of the CDP group to create or modify. The maximum number of characters supported is 32. Required.

Examples

Creating a CDP group named grp01:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match platform CISCO
switch(config-cdp-group)# match sw-version 11.2(12)P
switch(config-cdp-group)# match voice-vlan-query 512
switch(config-cdp-group)# seq 50 match platform cisco sw-version 11.2(12)P voice-
vlan-query 512
switch(config-cdp-group)# exit
switch(config)# do show running-config

Current configuration:
!
!Version AOS-CX Virtual.10.0X.000
!export-password: default
led locator on
!
!
vlan 1
port-access cdp-group grp01
     seq 10 match platform CISCO
     seq 20 match sw-version 11.2(12)P
     seq 30 match voice-vlan-query 512
     seq 50 match platform cisco sw-version 11.2(12)P voice-vlan-query 512
```

Removing a CDP group named grp01:

```
switch(config)# no port-access cdp-group grp01
```

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
6000 6100	config	Administrators or local user group members with execution rights for this command.

port-access device-profile

```
port-access device-profile <DEVICE-PROFILE-NAME>
no port-access device-profile <DEVICE-PROFILE-NAME>
```

Description

Creates a new device profile and switches to the **config-device-profile** context. A maximum of 32 device profiles can be created. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

The **no** form of this command removes a device profile.

Parameter	Description
<DEVICE-PROFILE-NAME>	Specifies the name of a device profile. Range: 1 to 32 alphanumeric characters.

Examples

Creating a device profile named **profile01**:

```
switch(config)# port-access device-profile profile01
switch(config-device-profile)#
```

Removing a device profile named **profile01**:

```
switch(config)# no port-access device-profile profile01
```

Creating a device profile named **profile02** on a LAG port:

```
switch(config)#interface lag 1
switch(config-lag-if)# port-access device-profile profile01
switch(config-device-profile)#
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-if`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

port-access device-profile mode block-until-profile-applied

You must configure this mode in device profile only on standalone ports where there is no security configured and when you not want the port to be offline until one client is onboarded.

```
port-access device-profile mode block-until-profile-applied
no port-access device-profile mode block-until-profile-applied
```

Description

Configures the switch to block the port until a profile match occurs for a device. This configuration is required when no security feature is enabled on the port.

You must enable this mode or security on the port for local MAC match feature to operate. You must not enable both features on the same port at the same time.

You must not combine any other AAA configurations with the block-until-profile-applied mode.

This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts. The **no** form of this command removes a rule for adding devices to a MAC group.

Example

Configuring block-until-profile applied mode on port 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access device-profile
switch(config-if-deviceprofile)# mode block-until-profile-applied
switch(config-if-deviceprofile)# end
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6000
6100
	`config-if`
	`config-if-deviceprofile`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

port-access lldp-group

```
port-access lldp-group <LLDP-GROUP-NAME>
no port-access lldp-group <LLDP-GROUP-NAME>
```

Description

Creates an LLDP group or modifies an existing LLDP group. An LLDP group is used to classify connected devices based on the LLDP type-length-values (TLVs) advertised by the device. A maximum of 32 LLDP groups can be configured on the switch. Each group accepts 64 match/ignore commands.

The **no** form of this command removes an LLDP group.

Parameter	Description
<LLDP-GROUP-NAME>	Specifies the name of the LLDP group to create or modify. The maximum number of characters supported is 32. Required.

Examples

Creating an LLDP group named grp01:

```
switch(config)# port-access lldp-group grp01
switch(config-lldp-group)#
```

Removing an LLDP group named grp01:

```
switch(config)# no port-access lldp-group grp01
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show port-access device-profile

```
show port-access device-profile [[interface {all | <INTERFACE-ID>}
     [client-status <MAC-ADDR>]] | name <DEVICE-PROFILE-NAME>]
```

Description

Shows the client status for a specific MAC address or profile name.

Parameter	Description
`interface {all | <INTERFACE-ID>}`	Select **all** for all interfaces or specify the name of an interface in the format: **member/slot/port**.
`client-status <MAC-ADDR>`	Specifies a MAC address (**xx:xx:xx:xx:xx:xx**), where **x** is a hexadecimal number from 0 to F.
`name <DEVICE-PROFILE-NAME>`	Specifies the name of the device profile.

Examples

Showing the applied state of the device profiles:

```
switch# show port-access device-profile

    Profile Name    : accesspoints
    LLDP Groups     : 2920-grp
    CDP Groups      :
    MAC Groups      : 2920-mac-grp1,2920-iot-grp2
    Role            : local_role_1
    State           : Enabled

    Profile Name    : access_switches
    LLDP Groups     : 2920-grp
    CDP Groups      :
    MAC Groups      :
    Role            : local_2920_role
```

```
    State           : Enabled

    Profile Name    : iot_devices
    LLDP Groups     :
    CDP Groups      :
    MAC Groups      : iot_camera-grp1,iot_sensors-grp1
    Role            : local_2920_role
    State           : Enabled

    Profile Name    : lobbyaps
    LLDP Groups     :
    CDP Groups      : lobby_ap_cdp_grp
    MAC Groups      :
    Role            : test_ap_role
    State           : Disabled
```

Showing the applied state of the device profile on interface 1/1/3:

```
switch# show port-access device-profile interface 1/1/3 client-status
00:0c:29:9e:d1:20

Port 1/1/3, Neighbor-Mac  00:0c:29:9e:d1:20
    Profile Name    : lobbyaps
    LLDP Group      :
    CDP Group       : aruba-ap_cdp
    MAC Group       :
    Role            : test_ap_role
    Status          : Failed
    Failure Reason  : Failed to apply MAC based VLAN
```

Showing the applied state of a specific device profile:

```
switch# show port-access device-profile name lldp-group

    Profile Name            : lldp-group
    LLDP Groups             :
    CDP Groups              :
    MAC Groups              : pc-behind-phone, lldp
    Role                    : auth_role
    State                   : 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
6000 6100	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 any interface VLAN to automatically obtain an IP address from a DHCP server on the network. By default, the DHCP client is enabled on VLAN 1.

The **no** form of the command disables DHCP mode and is supported only on interface VLANs.

Examples

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
```

If the interface is not enabled, you can enable it by entering the `no shutdown` command.

`ip dhcp` is supported only on one vlan at a time.

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-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)# interface vlan 1
switch(config-if-vlan)# ip dhcp option broadcast-flag
```

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)# interface vlan 1
switch(config-if-vlan)# no ip dhcp option host-name
```

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 Introduced

Command Information

Platforms	Command context	Authority
6000 6100	config-if-vlan	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,
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
10.13.1000	The output parameters, **Broadcast-flag** and **Hostname** 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.

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 this configuration is disabled, the DHCP relay agent on VTEPs ignores DHCP request packets that are received from client MACs addresses learned via EVPN.

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
6000 6100	config	Administrators or local user group members with execution rights for this command.

show dhcp-relay

```
show dhcp-relay
```

Description

Shows DHCP relay configuration settings.

Example

Showing DHCP relay settings:

```
switch(config)# show dhcp-relay

DHCP Relay Agent                  : enabled
DHCP Smart Relay                  : enabled
DHCP Request Hop Count Increment  : enabled
Option 82                         : enabled
Source-Interface                  : disabled
Response Validation               : disabled
Option 82 Handle Policy           : replace
Remote ID                         : mac

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
6000 6100	Manager (#)	Operators 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>]
```

Description

Shows the bootp gateway defined for all interfaces or a specific interface.

Parameter	Description
<INTERFACE-NAME>	Specifies an interface. Format: `member/slot/port`.

Examples

Showing the designated bootp gateway for all interfaces:

```
switch(config)# show dhcp-relay bootp-gateway

BOOTP Gateway Entries

Interface            Source IP
-------------------- ---------------
vlan10               1.1.1.1
vlan20               2.2.2.2
```

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
6000 6100	Manager (#)	Operators 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>]`

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`.

Examples

Showing the IP helper addresses for all interfaces:

```
switch(config)# show ip helper-address

IP Helper Addresses

Interface: vlan11
  IP Helper Address                  VRF
  -----------------                 -----------------
  10.10.10.209                       default

Interface: vlan20
  IP Helper Address                  VRF
  -----------------                 -----------------
  3.3.3.3                            default
  20.20.20.20                        default
```

Showing the IP helper addresses for interface vlan20:

```
switch(config)# show ip helper-address interface vlan20

IP Helper Addresses

Interface: vlan20
  IP Helper Address                  VRF
  -----------------                 -----------------
  3.3.3.3                            default
  20.20.20.20                        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
6000 6100	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show dhcpv6-relay

```
show dhcpv6-relay
```

Description

Shows DHCP relay configuration settings.

Example

```
switch# show dhcpv6-relay
  DHCPv6 Relay Agent : enabled
  Option 79          : disabled
  L2vpn-clients      : enabled
  Source-interface   : 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
	Manager (#)	Operators 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>]
```

Description

Shows the helper IP addresses defined for all interfaces or a specific interface.

Parameter	Description
`interface <INTERFACE-ID>`	Specifies an interface. Format: **member/slot/port**.

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
6000 6100	Manager (#)	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 dhcp-snooping binding

`clear dhcp-snooping binding {all | ip <IP-ADDR> vlan <VLAN-ID> | port <PORT-NUM> | vlan <VLAN-ID>}`

Description

Clears DHCP snooping binding entries.

Parameter	Description
`all`	Specifies that all DHCP binding information is to be cleared.
`ip <IP-ADDR> vlan <VLAN-ID>`	Specifies the IP address and VLAN for which all DHCP binding information is to be cleared.
`port <PORT-NUM>`	Specifies the port number for which all DHCP binding information is to be cleared.
`vlan <VLAN-ID>`	Specifies the VLAN for which all DHCP binding information is to be cleared.

Examples

Clearing all DHCP binding information for IP address 192.168.2.4 and VLAN 5:

```
switch(config)# clear dhcp-snooping binding ip 192.168.2.4 vlan 5
```

Clearing all DHCP binding information for port 1/1/1:

```
switch(config)# clear dhcp-snooping binding port 1/1/1
```

Clearing all DHCP binding information for VLAN 10:

```
switch(config)# clear dhcp-snooping binding vlan 10
```

Clearing all DHCP binding information:

```
switch(config)# clear dhcp-snooping binding all
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**. The **ipv4** parameter is deprecated and replaced with **ip**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 dhcp-snooping statistics

```
clear dhcp-snooping statistics
```

Description

Clears all DHCP snooping statistics.

Examples

Clear all DHCP snooping statistics:

```
switch# clear dhcp-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
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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-snooping

```
dhcp-snooping
no dhcp-snooping
```

Description

Enables DHCP snooping. DHCP snooping is disabled by default. DHCP snooping is not supported on the management interface.
The **no** form of the command disables DHCP snooping, flushing all the IP bindings learned since DHCP snooping was enabled.

Examples

Enabling DHCP snooping:

```
switch(config)# dhcp-snooping
```

Disabling DHCP snooping:

```
switch(config)# no dhcp-snooping
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping (in config-vlan context)

```
dhcp-snooping
no dhcp-snooping
```

Description

Enables DHCP snooping for the specified VLAN in the **config-vlan** context. DHCP snooping is disabled by default for all VLANs.

The no form of the command disables DHCP snooping on the specified VLAN, flushing all the IP bindings learned for this VLAN since DHCP snooping was enabled for this VLAN.

Examples

Enabling DHCP snooping on VLAN 100:

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

Disabling DHCP snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no dhcp-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
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	config-vlan	Administrators or local user group members with execution rights for this command.

dhcp-snooping allow-overwrite-binding

```
dhcp-snooping allow-overwrite-binding
no dhcp-snooping allow-overwrite-binding
```

Description

Allows binding to be overwritten for the same IP address. When enabled, and a DHCP server offers a host an IP address that is already bound to an existing host in the binding table, the existing binding is overwritten for the new host if the new host is successfully able to acquire the same IP address. This overwriting is disabled by default, causing the DHCP server offers to be dropped.

The **no** form of the command disables DHCP snooping overwrite binding.

Examples

Enabling DHCP snooping overwrite binding:

```
switch(config)# dhcp-snooping allow-overwrite-binding
```

Disabling DHCP snooping overwrite binding:

```
switch(config)# no dhcp-snooping allow-overwrite-binding
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping authorized-server

```
dhcp-snooping authorized-server <IP-ADDR> [vrf <VRF-NAME>]
no dhcp-snooping authorized-server <IP-ADDR> [vrf <VRF-NAME>]
```

Description

Adds an authorized (trusted) DHCP server to a list of authorized servers for use by DHCP snooping. This command can be issued multiple times, adding a maximum of 20 authorized servers per VRF. By default, with an empty list of authorized servers, all DHCP servers are considered to be trusted for DHCP snooping purposes.

The **mgmt** VRF cannot be used with this command.

The no form of this command deletes the specified DHCP server from the authorized list.

Parameter	Description
<IP-ADDR>	Specifies the IP address of the trusted DHCP server.
`vrf` *<VRF-NAME>*	Specifies the VRF name.

Usage

For authorized server lookup, the VRF is derived from the Switch Virtual Interface (SVI) configured for the incoming VLAN. If the SVI is not configured, the `default` VRF is assumed.

Examples

Adding DHCP servers 192.168.2.2, 192.168.2.3, and 192.168.2.10 to the authorized server list:

```
switch(config)# dhcp-snooping authorized-server 192.168.2.2
switch(config)# dhcp-snooping authorized-server 192.168.2.3 vrf default
switch(config)# dhcp-snooping authorized-server 192.168.2.10 vrf default
```

Removing DHCP server 192.168.2.3 from the authorized server list:

```
switch(config)# no dhcp-snooping authorized-server 192.168.2.3 vrf default
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping event-log client

```
dhcp-snooping event-log client
no dhcp-snooping event-log client
```

Description

This command enables or disables dhcp-snooping client level event logs that help with client telemetry on a remote management station such as Aruba Central. By default, client level event logs are disabled. The **no** form of this command disables client-level event logs for DHCP snooping after they are enabled. View these logged DHCP snooping events by issuing the command **show events -c dhcp-snooping**.

For additional information on DHCP-related event logging, please refer to the Event Log Message Reference Guide.

Examples

Enabling DHCP client level event logs:

```
switch(config)# # dhcp-snooping event-log client
```

Disabling external storage:

```
witch(config)# # no dhcp-snooping event-log client
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping external-storage

```
dhcp-snooping external-storage volume <VOL-NAME> file <FILE-NAME>
no dhcp-snooping external-storage volume <VOL-NAME> file <FILE-NAME>
```

Description

Configures external storage to be used for backing up IP bindings (used by DHCP snooping) to a file. When configured, the switch stores all the IP bindings in an external storage file so that they are retained after the switch restarts. When the switch restarts, it reads the IP bindings from the configured external storage file to populate its local cache.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IP bindings in an external storage file.

Parameter	Description
`volume <VOL-NAME>`	Specifies the name of the existing external storage volume where the IP bindings file will be saved. Before running the **dhcp-snooping external-storage volume** command, first create the external storage volume using command **external-storage <VOLUME-NAME>**. See *External storage commands* in the *Command-Line Interface Guide*.
`file <FILE-NAME>`	Specifies the file name to use for storing IP bindings. Maximum 255 characters.

Configuring IP bindings storage in file **dsnoop_ipbindings** on existing volume **dhcp_snoop**:

```
switch(config)# dhcp-snooping external-storage volume dhcp_snoop file dsnoop_
ipbindings
```

Disabling external storage:

```
switch(config)# no dhcp-snooping external-storage volume dhcp_snoop
```

Disabling external storage when flash storage is also configured (note the message indicating that flash storage will be used):

```
switch(config)# no dhcp-snooping external-storage volume dhcp_snoop
dhcp-snooping will use flash storage to store IP Binding database
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
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping flash-storage

```
dhcp-snooping flash-storage [delay <DELAY>]
no dhcp-snooping flash-storage [delay <DELAY>]
```

Description

Configures switch flash storage to be used for backing up client IP bindings (used by DHCP snooping). When flash storage is configured (and external storage is not already configured for this purpose), the switch stores the IP bindings in switch flash storage. When the switch restarts, it reads the IP bindings from the switch flash storage to populate its local cache.

Writing the IP bindings to flash storage only occurs after the configured delay and if there has been a change in client IP bindings. Writing is skipped when client IP bindings have not changed since the previous write.

Omitting **delay <DELAY>** sets the default delay of 900 seconds.

To reduce switch flash aging it is recommended that you use external storage (command **dhcp-snooping external-storage**) to backup DHCP snooping IP bindings. Alternatively, consider configuring flash storage with a substantial delay between writes.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IP bindings in flash storage.

Parameter	Description
`delay <DELAY>`	Specifies the delay in seconds between writes (when necessary) to the flash storage, Default: 900. Range: 300 to 86400.

Examples

Configuring switch flash storage for DHCP snooping IP binding storage with a write delay of 1200 seconds:

```
switch(config)# dhcp-snooping flash-storage delay 1200
Warning: Using flash storage reduces switch lifetime. It is recommended to use an
external-storage.
Do you want to continue  (y/n)? y
switch(config)#
```

Unconfiguring usage of switch flash storage for IP bindings :

```
switch(config)# no dhcp-snooping flash-storage
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	config	Administrators or local user group members with execution rights for this command.

dhcp-snooping max-bindings

```
dhcp-snooping max-bindings <MAX-BINDINGS>
no dhcp-snooping max-bindings <MAX-BINDINGS>
```

Description

Sets the maximum number of DHCP bindings allowed on the selected interface. For all interfaces on which this command is not run, the default max binding is the maximum value of the range.

The no form of the command reverts max bindings for the selected interface to its default.

Parameter	Description
<MAX-BINDINGS>	Specifies the maximum number of DHCP bindings. Range: 1 to 256.

Examples

Set the DHCP max bindings to 256 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# dhcp-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

Revert DHCP max bindings to its default on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no dhcp-snooping max-bindings 256
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
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

dhcp-snooping option 82

```
dhcp-snooping option 82 [remote-id {mac | subnet-ip}]
                        [untrusted-policy {drop | keep | replace}]
no dhcp-snooping option 82 [remote-id {mac | subnet-ip}]
                        [untrusted-policy {drop | keep | replace}]
```

Description

Configures the addition of option 82 DHCP relay information to DHCP client packets that are being forwarded on trusted ports. DHCP relay is enabled by default.

In the switch default state and when this command is entered without parameters (**dhcp-snooping option 82**), this default configuration is used:

```
dhcp-snooping option 82 remote-id mac untrusted-policy drop
```

When **remote-id** is omitted, its default (**mac**) is used. When **untrusted-policy** is omitted, its default (**drop**) is used.

The no form of this command disables DHCP snooping option 82.

Parameter	Description
`remote-id`	Specifies what address to use as the remote ID for the `replace` option of `untrusted-policy`. Specify one of these address types:

Parameter	Description
`mac`	The default. Uses the switch MAC address as the remote ID.
`subnet-ip`	Uses the IP address of the client VLAN as the remote ID.
`untrusted-policy`	Specifies what action to take for DHCP packets (with option 82) that are received on untrusted ports. Specify one of these actions:
`drop`	The default. Drop DHCP packets (with option 82) without forwarding them.
`keep`	Forward DHCP packets (with option 82).
`replace`	Replace the option 82 information in the DHCP packets with whatever is set for **remote-id** (one of: **mac**, **subnet-ip**, or **mgmt-ip**) and forward the packets.

Examples

Configuring DHCP snooping option 82 with the keep action:

```
switch(config)# dhcp-snooping option 82 untrusted-policy keep
```

Disabling DHCP snooping option 82:

```
switch(config)# no dhcp-snooping option 82 untrusted-policy keep
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping static-attributes

```
dhcp-snooping static-attributes
no dhcp-snooping static-attributes
```

Description

Enables storage of static attributes provided to the DHCP client by DHCP server during DHCP packet exchange. Disabled by default. When enabled, the following attributes are stored in OVSDB along with the client IP binding entry:

1. Name server IP addresses: DNS server IPs provided by the DHCP server to the client. Maximum: 3 per client.
2. Default gateway IP address: Router IP addresses provided by DHCP server to the client. Maximum: 3 per client.
3. Server IP address: IP address of the DHCP server that leased the IP to the client.

The **no** form of the command disables storing of client static attributes. After disabling, existing client static attributes will be flushed.

Examples

Enabling the storage of DHCP snooping static attributes:

```
switch(config)# dhcp-snooping static-attributes
```

Disabling the storage of DHCP snooping static attributes:

```
switch(config)# no dhcp-snooping static-attributes
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcp-snooping trust

```
dhcp-snooping trust
no dhcp-snooping trust
```

Description

Enables DHCP snooping trust on the selected port. Only server packets received on trusted ports are forwarded. All the ports are untrusted by default.

The **no** form of the command disables DHCP snooping trust on the selected port.

Examples

Enabling DHCP snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# dhcp-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling DHCP snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no dhcp-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
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

dhcp-snooping verify mac

```
dhcp-snooping verify mac
no dhcp-snooping verify mac
```

Description

This command enables verification of the hardware address field in DHCP client packets. When enabled, the DHCP client hardware address field and the source MAC address must be the same for packets

received on untrusted ports or else the packet is dropped. This DHCP snooping MAC verification is enabled by default.

The **no** form of the command disables DHCP snooping MAC verification.

Examples

Enabling DHCP snooping MAC verification:

```
switch(config)# dhcp-snooping verify mac
```

Disabling DHCP snooping MAC verification:

```
switch(config)# no dhcp-snooping verify mac
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show dhcp-snooping

`show dhcp-snooping`

Description

Shows the DHCP snooping configuration.

Examples

Showing the DHCP snooping configuration:

```
switch# show dhcp-snooping
```

```
dhcp-snooping Information

dhcp-snooping                  : Yes             Verify MAC Address   : Yes
Allow Overwrite Binding        : No              Enabled VLANs        : 1-100
Static Attributes              : Yes
Client Event Logs              : Yes

Option 82 Configurations

Untrusted Policy               : replace          Insertion           : Yes
Option 82 Remote-id            : mac

External Storage Information

Volume Name    : ipbinding
File Name      : ipv4Bindings
Inactive Since : 01:23:20 09/10/2021
Error          : File Write Failure

Flash Storage Information

File Write Delay : 300 seconds
Active Storage   : External

Authorized Server Configurations

VRF                            Authorized Servers
------------                  ----------------------
default                        1.1.10.3
default                        10.10.10.1
default                        10.10.10.56
default                        200.10.10.3
green                          1.1.10.3
green                          1.10.10.3
green                          10.10.100.3
red                            192.168.122.53
red                            192.168.122.121

Port Information

                      Max          Static      Dynamic
Port        Trust     Bindings     Bindings    Bindings
--------    -----      --------    --------      --------
1/1/2       Yes         5000        50            0
1/1/3       Yes         8192        0             0
1/1/5       Yes         8192        0             22
1/1/16      No          100         0             0
10/10/10    No          8100        320           200
lag120      No          512         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
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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-snooping binding

```
show dhcp-snooping binding
```

Description

Shows the DHCP snooping binding configuration.

Parameter	Description
`detail`	Shows detailed information for active IP bindings on the system.

Examples

Showing the DHCP snooping binding configuration:

```
switch(config)# show dhcp-snooping binding

  MacAddress         IP              VLAN  Interface  Time-Left
  -----------------  --------------  ----  ---------  ---------
  aa:b1:c1:dd:ee:ff  10.2.3.4        1     1/1/2      582
  aa:b2:c2:dd:ee:ff  10.2.3.5        1     1/1/2      584
```

Showing detailed information for active IP bindings:

```
switch(config)# show dhcp-snooping binding detail

VLAN Id : 2, MAC : 00:50:56:96:74:46

  IP               Interface  Time-Left
  ---------------  ---------  -------------------
  100.1.2.100      1/1/23     194

  Static Attributes:
  Default Router  : 100.1.2.1, 192.1.1.1, 1.1.1.2
  Server IP       : 10.1.84.2
```

```
  Name Servers    : 192.1.1.2, 2.2.2.2, 1.1.1.1


VLAN Id : 3, MAC : 00:50:56:96:e5:8e

  IP               Interface  Time-Left
  ---------------  ---------  -------------------
  100.1.3.100      2/1/22     145

  Static Attributes:
  Default Router   : 100.1.3.1, 192.1.1.1, 1.1.1.2
  Server IP        : 10.1.84.2
  Name Servers     : 192.1.1.2, 2.2.2.2, 1.1.1.1

VLAN Id : 3, MAC : 00:11:01:00:00:03

  IP               Interface  Time-Left
  ---------------  ---------  -------------------
  100.1.3.99       2/1/24     137

  Static Attributes:
  Default Router   : 100.1.3.1, 192.1.1.1, 1.1.1.2
  Server IP        : 10.1.84.2
  Name Servers     :192.168.0.1, 192.168.1.1, 192.168.2.1
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.14	The **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.10	Detail parameter added.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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-snooping statistics

`show dhcp-snooping statistics`

Description

Shows the DHCP snooping statistics.

Examples

Showing the DHCP snooping statistics:

```
switch(config)# show dhcp-snooping statistics

 Packet-Type  Action   Reason                          Count
 -----------  -------  ------------------------------  ---------
 server       forward  from trusted port               5425
 client       forward  to trusted port                 3895
 server       drop     received on untrusted port      117
 server       drop     unauthorized server             214
 client       drop     destination on untrusted port   78
 client       drop     untrusted option 82 field       85
 client       drop     bad DHCP release request        0
 client       drop     failed verify MAC check         5
 client       drop     failed on max-binding limit     15
```

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 **dhcpv4-snooping** keyword is deprecated and replaced with **dhcp-snooping**.
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 dhcpv6-snooping binding

`clear dhcpv6-snooping binding {all | ip <IPV6-ADDR> vlan <VLAN-ID> | interface <IFNAME> | vlan <VLAN-ID>}`

Description

Clears DHCPv6 snooping binding entries.

Parameter	Description
`all`	Specifies that all DHCPv6 binding information is to be cleared.
`ip <IPV6-ADDR> vlan <VLAN-ID>`	Specifies the IPv6 address and VLAN for which all DHCPv6 binding information is to be cleared.
`interface <IFNAME>`	Specifies the interface for which all DHCPv6 binding information is to be cleared.
`vlan <VLAN-ID>`	Specifies the VLAN for which all DHCPv6 binding information is to be cleared. Range: 1 to 4094.

Examples

Clearing all DHCPv6 binding information for 5000::1 vlan 1:

```
switch(config)# clear dhcpv6-snooping binding ip 5000::1 vlan 1
```

Clearing all DHCPv6 binding information for interface 1/1/10:

```
switch(config)# clear dhcpv6-snooping binding interface 1/1/10
```

Clearing all DHCPv6 binding information for VLAN 10:

```
switch(config)# clear dhcpv6-snooping binding vlan 10
```

Clearing all DHCPv6 binding information:

```
switch(config)# clear dhcpv6-snooping binding all
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 dhcpv6-snooping statistics

`clear dhcpv6-snooping statistics`

Description

Clears all DHCPv6 snooping statistics.

Examples

Clear all DHCPv6 snooping statistics:

```
switch# clear dhcpv6-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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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-snooping

```
dhcpv6-snooping
no dhcpv6-snooping
```

Description

Enables DHCPv6 snooping. DHCPv6 snooping is disabled by default. DHCPv6 snooping is not supported on the management interface.

The no form of the command disables DHCPv6 snooping, flushing all the IP bindings learned since DHCPv6 snooping was enabled.

Examples

Enabling DHCPv6 snooping:

```
switch(config)# dhcpv6-snooping
```

Disabling DHCPv6 snooping:

```
switch(config)# no dhcpv6-snooping
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping (in config-vlan context)

```
dhcpv6-snooping
no dhcpv6-snooping
```

Description

Enables DHCPv6 snooping in the `config-vlan` context. DHCPv6 snooping is disabled by default for all VLANs.

The no form of the command disables DHCPv6 snooping on the specified VLAN, flushing all the IPv6 bindings learned for this VLAN since DHCPv6 snooping was enabled for this VLAN.

Examples

Enabling DHCPv6 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# dhcpv6-snooping
switch(config-vlan-100)# exit
switch(config)#
```

Disabling DHCPv6 snooping on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# no dhcpv6-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
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	`config-vlan`	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping authorized-server

`dhcpv6-snooping authorized-server <IPV6-ADDR> [vrf <VRF-NAME>]`
`no dhcpv6-snooping authorized-server <IPV6-ADDR> [vrf <VRF-NAME>]`

Description

Adds an authorized (trusted) DHCPv6 server to a list of authorized servers for use by DHCPv6 snooping. This command can be issued multiple times, adding a maximum of 20 authorized servers per VRF. By default, with an empty list of authorized servers, all DHCPv6 servers are considered to be trusted for DHCPv6 snooping purposes.

The `mgmt` VRF cannot be used with this command.

Configure the link local IPv6 address instead of global IPv6 address of the DHCPv6 server as the authorized-server. For example:

```
switch(config)# dhcpv6-snooping authorized-server fe80::2ca4:fa40:d4cd:bc2f
```

The no form of this command deletes the specified DHCPv6 server from the authorized list.

Parameter	Description
<IPV6-ADDR>	Specifies the IPv6 address of the trusted DHCPv6 server.
`vrf` *<VRF-NAME>*	Specifies the VRF name.

Usage

For authorized server lookup, the VRF is derived from the Switch Virtual Interface (SVI) configured for the incoming VLAN. If the SVI is not configured, the `default` VRF is assumed.

Examples

Adding DHCP servers ABCD:5ACD::2000, and ABCD:5ACD::2010 to the authorized server list:

```
switch(config)# dhcpv6-snooping authorized-server ABCD:5ACD::2000 vrf default
switch(config)# dhcpv6-snooping authorized-server ABCD:5ACD::2010 vrf default
```

Removing DHCP server ABCD:5ACD::2000 from the authorized server list:

```
switch(config)# no dhcpv6-snooping authorized-server ABCD:5ACD::2000 vrf default
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping event-log client

`dhcpv6-snooping event-log client`

```
no dhcpv6-snooping event-log client
```

Description

This command enables or disables DHCPv6 snooping client level event logs that help with client telemetry on a remote management station such as Aruba Central. By default, client level event logs are disabled. The **no** form of this command disables client-level event logs for DHCPv6 snooping after they are enabled. View these logged DHCPv6 snooping events by issuing the command `show events -c dhcpv6-snooping`.

For additional information on DHCP-related event logging, please refer to the Event Log Message Reference Guide.

Examples

Enabling DHCPv6 client level event logs:

```
switch(config)# # dhcpv6-snooping event-log client
```

Disabling external storage:

```
witch(config)# # no dhcpv6-snooping event-log client
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping external-storage

```
dhcpv6-snooping external-storage volume <VOL-NAME> file <FILE-NAME>
no dhcpv6-snooping external-storage volume <VOL-NAME> file <FILE-NAME>
```

Description

Configures external storage to be used for backing up IPv6 bindings (used by DHCPv6 snooping) to a file. When configured, the switch stores all the IP bindings in an external storage file so that they are retained after the switch restarts. When the switch restarts, it reads the IPv6 bindings from the configured external storage file to populate its local cache.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IPv6 bindings in an external storage file.

Parameter	Description
`volume <VOL-NAME>`	Specifies the name of the existing external storage volume where the IPv6 bindings file will be saved. Before running the `dhcpv6-snooping external-storage volume` command, first create the external storage volume using command `external-storage <VOLUME-NAME>`. See *External storage commands* in the *Command-Line Interface Guide*.
`file <FILE-NAME>`	Specifies the file name to use for storing IPv6 bindings. Maximum 255 characters.

Examples

Configuring IPv6 bindings storage in file `ipv6Bindings` on existing volume `dhcp_snoop`:

```
switch(config)# dhcpv6-snooping external-storage volume dhcp_snoop file
ipv6Bindings
```

Disabling external storage:

```
switch(config)# no dhcpv6-snooping external-storage volume dhcp_snoop
```

Disabling external storage when flash storage is also configured (note the message indicating that flash storage will be used):

```
switch(config)#  no dhcpv6-snooping external-storage volume dhcp_snoop
DHCPv6-Snooping will use flash storage to store IP Binding database
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
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping flash-storage

```
dhcpv6-snooping flash-storage [delay <DELAY>]
no dhcpv6-snooping flash-storage [delay <DELAY>]
```

Description

Configures switch flash storage to be used for backing up client IP bindings (used by DHCPv6 snooping). When flash storage is configured (and external storage is not already configured for this purpose), the switch stores the IP bindings in switch flash storage. When the switch restarts, it reads the IP bindings from the switch flash storage to populate its local cache.

Writing the IP bindings to flash storage only occurs after the configured delay and if there has been a change in client IP bindings. Writing is skipped when client IP bindings have not changed since the previous write.

Omitting `delay <DELAY>` sets the default delay of 900 seconds.

To reduce switch flash aging it is recommended that you use external storage (command `dhcpv6-snooping external-storage`) to backup DHCP snooping IP bindings. Alternatively, consider configuring flash storage with a substantial delay between writes.

When both external storage and flash storage are configured to store DHCP snooping IP bindings, the external storage takes priority, and is used exclusively until it becomes unconfigured, at which time flash storage (if configured) is used. Later, if external storage is configured again, flash storage stops and external storage resumes.

The no form of this command disables the saving of IP bindings in flash storage.

Parameter	Description
`delay <DELAY>`	Specifies the delay in seconds between writes (when necessary) to the flash storage, Default: 900. Range: 300 to 86400.

Examples

Configuring switch flash storage for DHCP snooping IP binding storage with a write delay of 1200 seconds:

```
switch(config)# dhcpv6-snooping flash-storage delay 1200
Warning: Using flash storage reduces switch lifetime. It is recommended to use an
external-storage.
Do you want to continue  (y/n)? y
switch(config)#
```

Unconfiguring usage of switch flash storage for IP bindings :

```
switch(config)# no dhcpv6-snooping flash-storage
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	config	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping max-bindings

```
dhcpv6-snooping max-bindings <MAX-BINDINGS>
no dhcpv6-snooping max-bindings <MAX-BINDINGS>
```

Description

Sets the maximum number of DHCPv6 bindings allowed on the selected interface. For all interfaces on which this command is not run, the default max binding is the maximum value of the range.

The no form of the command reverts max bindings for the selected interface to its default.

Parameter	Description
<MAX-BINDINGS>	Specifies the maximum number of DHCP bindings. Range: 1 to 256.

Examples

Set the DHCPv6 max bindings to 256 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# dhcpv6-snooping max-bindings 256
switch(config-if)# exit
switch(config)#
```

Revert DHCPv6 max bindings to its default on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no dhcpv6-snooping max-bindings 256
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
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

dhcpv6-snooping trust

```
dhcpv6-snooping trust
no dhcpv6-snooping trust
```

Description

Enables DHCPv6 snooping trust on the selected interface. Only server packets received on trusted interfaces are forwarded. All the interfaces are untrusted by default.

The no form of the command disables DHCPv6 snooping trust on the selected interface.

`config-if`

Examples

Enabling DHCPv6 snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# dhcpv6-snooping trust
switch(config-if)# exit
switch(config)#
```

Disabling DHCPv6 snooping trust on interface 2/2/1:

```
switch(config)# interface 2/2/1
switch(config-if)# no dhcpv6-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
10.09	Command introduced for the 6000 and 6100 Switch Series.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show dhcpv6-snooping

```
show dhcpv6-snooping
```

Description

Shows the DHCPv6 snooping configuration.

Examples

Showing the DHCPv6 snooping configuration:

```
switch# show  dhcpv6-snooping

 DHCPv6-Snooping Information

  DHCPv6-Snooping      : Yes   Enabled VLANs        : 1,5,7,100-110
  Trusted Port Bindings Enabled VLANs :
  Client Event Logs                  : Yes

External Storage Information

   Volume Name           : dhcp_snoop
   File Name             : ip_binding
   Inactive Since        : 01:23:20 09/10/2021
   Error                 : Failed to write external storage

Flash Storage Information
     File Write Delay       : 300 seconds
     Active Storage         : External

Authorized Server Configurations
VRF                                        Authorized Servers
------------                              ------------------
default
2001:0db8:85a3:0000:0000:8a2e:0370:7334
default                                    2002::2
default                                    2004::1
red                                        2002::1
red                                        2002::2
red                                        2002::9
green                                      5000::1
green                                      5000::2
green                                      5000::3
green                                      5000::7
green                                      5000::8
```

```
Port Information
                          Max       Static      Dynamic
Port            Trust     Bindings  Bindings    Bindings
--------        -----     --------   --------  --------
1/1/2           Yes       0         0         0
1/1/3           Yes       0         3         0
1/1/5           Yes       0         22        0
1/1/16          No        256       0         20
10/10/10        No        256       12        7
lag120          No        256       3         0
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.08	Updated example with flash storage information.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show dhcpv6-snooping binding

`show dhcpv6-snooping binding`

Description

Shows the DHCPv6 snooping binding configuration.

Examples

Showing the DHCPv6 snooping binding configuration:

```
switch# show dhcpv6-snooping binding

 IP Binding Information
 ======================
 MAC-ADDRESS       IPV6-ADDRESS                                VLAN  INTERFACE
TIME-LEFT
 ----------------  ------------------------------------------  ----  ---------  ----
------
 00:50:56:96:e4:cf aaaa:bbbb:cccc:dddd:eeee:1234:5678:abcd      1      1/1/1
  584
 00:50:56:96:04:4d 1000::3                                     134      1/1/2
  435
```

```
 00:50:56:96:d8:3d 2000:1000::4                                  2002     lag123
21234
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show dhcpv6-snooping statistics

```
show dhcpv6-snooping statistics
```

Description

Shows the DHCPv6 snooping statistics.

Examples

Showing the DHCPv6 snooping statistics:

```
switch(config)# show dhcpv6-snooping statistics

 Packet-Type  Action   Reason                          Count
 -----------  -------  ------------------------------  ---------
 server       forward  from trusted port               12
 client       forward  to trusted port                 20
 server       drop     received on untrusted port      5
 server       drop     unauthorized server             4
 client       drop     destination on untrusted port   2
 client       drop     bad DHCP release request        5
 server       drop     relay reply on untrusted port   2
 client       drop     failed on max-binding limit     5
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.09.1000	Command introduced for the 8360 Switch Series.
10.09	Command introduced for the 6000 and 6100 Switch Series.
10.07 or earlier	

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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-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:

```
switch(config)# http-proxy http-proxy.aruba.com vrf mgmt
switch(config)# http-proxy [2000::100]: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 default]
no ip dns domain-list <DOMAIN-NAME> [vrf default]
```

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
`list <DOMAIN-NAME>`	Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.

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 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
<DOMAIN-NAME>	Specifies the domain name to append to DNS requests. Length: 1 to 256 characters.
`vrf` *<VRF-NAME>*	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 (**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.
`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 (**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.
`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.

show ip dns

`show ip dns [vrf <VRF-NAME>]`

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.

Examples

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 enties).

AOS-CX gives the following priority levels to the these three update mothods.

- Priority 1 - standalone CLI configuration
- Priority 2 - static ip dns configuration
- Priority 3 - Dynamic config

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.

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.

(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:
	`excessive-broadcasts`
	`excessive-multicasts`
	`excessive-link-flaps`
	`excessive-oversize-packets`
	`excessive-jabbers`
	`excessive-fragments`
	`excessive-crc-errors`
	`excessive-late-collisions`
	`excessive-collisions`
	`excessive-tx-drops`
	`excessive-alignment-errors`

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-late-collisions
switch(config-fault-monitor-profile)# excessive-collisions
switch(config-fault-monitor-profile)# excessive-tx-drops
switch(config-fault-monitor-profile)# excessive-alignment-errors
```

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-late-collisions
switch(config-fault-monitor-profile)# no excessive-collisions
switch(config-fault-monitor-profile)# no excessive-tx-drops
switch(config-fault-monitor-profile)# no excessive-alignment-errors
```

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-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:
	`excessive-broadcasts`
	`excessive-multicasts`
	`excessive-link-flaps`
	`excessive-oversize-packets`
	`excessive-jabbers`
	`excessive-fragments`
	`excessive-crc-errors`
	`excessive-late-collisions`
	`excessive-collisions`
	`excessive-tx-drops`
	`excessive-alignment-errors`

`notify`	Selects the `notify` action. Notifies through events, DLOGs, and SNMP trap. This action is enabled by default.
`notify-and-disable`	Selects the action as `notify-and-disable`. 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 `notify-and-disable` 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-late-collisions action notify-and-
disable
switch(config-fault-monitor-profile)# excessive-collisions action notify-and-
disable
```

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
switch(config-fault-monitor-profile)# excessive-alignment-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-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
switch(config-fault-monitor-profile)# no excessive-collisions 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
10.07 or earlier	--

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
10.08	Made the *<PROFILE-NAME>* parameter optional in the **no** form of the command.
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.

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
10.07 or earlier	--

Command Information

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

show 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-late-collisions       yes      25          notify-and-disable  --
excessive-collisions            yes      25          notify-and-disable  --
excessive-tx-drops              yes      25          notify-and-disable  --
excessive-alignment-errors      yes      25          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-late-collisions       yes      30          notify-and-disable  --
excessive-collisions            yes      30          notify-and-disable  --
excessive-tx-drops              yes      30          notify-and-disable  --
excessive-alignment-errors      yes      30          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-late-collisions       yes      25          notify-and-disable  --
excessive-collisions            yes      25          notify-and-disable  --
excessive-tx-drops              yes      25          notify-and-disable  --
excessive-alignment-errors      yes      25          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
10.07 or earlier	--

Command Information

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

show 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
10.07 or earlier	--

Command Information

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

show 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  Time
Port   Fault                        Fault Elapsed Time            State 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  Time
Port   Fault                        Occurring Since               State 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
10.07 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 [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-late-collisions
    excessive-late-collisions threshold value 25
    excessive-late-collisions action notify
    no excessive-collisions
    excessive-collisions threshold value 25
    excessive-collisions action notify
    no excessive-tx-drops
    excessive-tx-drops threshold value 25
    excessive-tx-drops action notify
    no excessive-alignment-errors
    excessive-alignment-errors threshold value 25
    excessive-alignment-errors action notify
...
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
10.07 or earlier	--

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

`<FAULT> threshold value <VALUE>`
 	
With `<FAULT>` set to any of these names:
`excessive-oversize-packets`
`excessive-jabbers`
`excessive-fragments`
`excessive-crc-errors`
`excessive-late-collisions`
`excessive-collisions`
`excessive-tx-drops`
`excessive-alignment-errors`
	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.

`excessive-link-flaps` `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-broadcasts |`
`excessive-multicasts}`
`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 |`
`excessive-multicasts}`
`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-late-collisions threshold value 30
switch(config-fault-monitor-profile)# excessive-collisions threshold value 40
```

```
switch(config-fault-monitor-profile)# excessive-tx-drops threshold value 20
switch(config-fault-monitor-profile)# excessive-alignment-errors threshold value
50

switch(config-fault-monitor-profile)# excessive-link-flaps threshold count 14
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-late-collisions threshold
switch(config-fault-monitor-profile)# no excessive-collisions threshold
switch(config-fault-monitor-profile)# no excessive-tx-drops threshold
switch(config-fault-monitor-profile)# no excessive-alignment-errors threshold

switch(config-fault-monitor-profile)# no excessive-link-flaps 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
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-fault-monitor-profile`	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. Required

<REMOTE-URL>	Specifies the URL to receive the uploaded firmware using SFTP , TFTP or SCP.
	TFTP format:
	`tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME>`
	SFTP format:
	`sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME>`
	SCP format:
	`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 **usb:/**. For example: **usb:/firmware_v1.2.3.swi** 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>	Specifies the URL from which to download the firmware using SFTP or TFTP. **TFTP format:**

Parameter	Description

	`tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME>`
	SFTP format:
	`sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME>`
	SCP format:
	`scp://USER@{IP|HOST}[:PORT]/FILE`

`{hot-patch|primary|secondary}`	Select a hot-patch or a primary or secondary image profile for receiving the downloaded firmware. Required. **NOTE:** For more information about hot-patch, see hot-patch.
`vrf <VRF-NAME>`	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 `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 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 default
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 device. Required. **USB format:** `usb:/<FILENAME>`
`{hot-patch|primary|secondary}`	Select a hot-patch image or a primary or secondary profile for receiving the copied firmware. **NOTE:** For more information about hot-patch, see hot-patch.

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
<Word>	Name of the hot-patch software to upload.
<REMOTE-URL>	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.
`vrf <VRF-NAME>`	[Optional] specify the VRF instance to use for upload.
<STORAGE-URL>	Specifies the name of the patch file to create on the USB storage device. Prefix the filename with **usb:/**, for example, **usb:/firmware_FL_10_12_0001-0002.patch.**

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
copy <REMOTE-URL>	Downloads a hot-patch image from a TFTP or SFTP server.
hot-patch	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
`apply <name.patch>`	Apply the specified hot-patch image to a standalone switch or VSF stack. AOS-CX hot-patch software images can be obtained from Aruba customer support, and are identified with a **.patch** extension.
`remove <name.patch>`	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
copy <REMOTE-URL>	Downloads and installs a hot-patch image from a TFTP or SFTP server.
copy hot-patch	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            : ArubaOS-CX:FL.10.12.0001-sp1-256-gd457e868d39:202204142009
Patch SHA           : a40438d06a82e5fe7e30d457e868d39e8526185b
```

Related Commands

Command	Description
copy <REMOTE-URL>	Downloads a hot-patch image from a TFTP or SFTP server.
hot-patch	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.

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

Enables the firmware site distribution server.

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.

Example

Enabling the firmware site distribution server:

```
switch(config)# https-server rest firmware-site-distribution
```

Disabling the firmware site distribution server:

```
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.

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.

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 maxium 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 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.

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.

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

show https-server

`show https-server`

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.

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
6000 6100	Operator (>) or Manager (#)	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 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
<PACKET-INTERVAL>	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 *<PACKET-INTERVAL>* parameter to the **no** 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 packed. 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-vlan`.

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
```

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
All platforms	`config-if-vlan`	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
`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 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	`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	`config-if-vlan`	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
```

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
All platforms	`config-if-vlan`	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
```

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
All platforms	config-if-vlan	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:

```
6200-1(config-if-vlan)# ip igmp querier-wait-time
<1-300>  Querier Wait value (Default: 260)
6200-1(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	`config-if-vlan`	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	`config-if-vlan`	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	`config-if-vlan`	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	`config-if-vlan`	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	`config-if-vlan`	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
```

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	`config-if-vlan`	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	`config-if-vlan`	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
```

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
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

show ip igmp

```
show ip igmp [all-vrfs]
```

Description

Shows IGMP configuration information and status, or shows information by VRF.

Parameter	Description
`all-vrfs`	To show information for all VRFs, specify **all-vrfs**.

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 all VRFs:

```
switch# show ip igmp all-vrfs
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
```

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	Operator (>) or Manager (#)	Operators 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 [all-vrfs]`

Description

Shows IGMP counter details, or shows counters by VRF.

Parameter	Description
`all-vrfs`	Specify **all-vrfs** to show information for all VRFs.

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	Operator (>) or Manager (#)	Operators 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>] [all-vrfs]`

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
all-vrfs	Specify **all-vrfs** to show information for all VRFs.

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

                              V1         V2         Sources   Sources
Vers Mode Uptime    Expires   Timer      Timer      Forwarded Blocked
---- ---- --------- --------- ---------- ---------- --------- --------
3    EXC  16m 34s   2m 27s
```

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
```

```
                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  17m 5s    4m 2s
```

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

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  17m 35s   3m 32s
```

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	Operator (>) or Manager (#)	Operators 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 [all-vrfs]
```

Description

Shows IGMP group information, or you can display group information by VRF.

Parameter	Description
`all-vrfs`	Specify **all-vrfs** to show information for all VRFs.

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

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 36s    3m 44s

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

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 36s    3m 44s
```

Showing IGMP groups for all VRFs:

```
switch# show ip igmp groups all-vrfs
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

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded 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

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded 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

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded 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

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded 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

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded 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

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded 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	Operator (>) or Manager (#)	Operators 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 [{{vlan <VLAN-ID>}]
counters
group <A.B.C.D> [{source <A.B.C.D>}|
groups
statistics
```

Description

Shows IGMP configuration information for a specific interface (VLAN).

Parameter	Description
`vlan <VLAN-ID>`	Specifies a VLAN. Values: 1-4094.

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
```

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
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 igmp interface counters

`show ip igmp interface { vlan <VLAN-ID>} counters`

Description

Shows IGMP counter details for a specific interface or VLAN interface.

Parameter	Description
`vlan <VLAN-ID>`	Specifies a VLAN. Values: 1-4094.

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
```

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
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 igmp interface group

`show ip igmp [interface { vlan <VLAN-ID>} [group <GROUP-IP> [source <SOURCE-IP>]]]`

Description

Shows IGMP joined group information for a specific interface or VLAN interface, or specify a source IP.

Parameter	Description
`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

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

                              V1         V2         Sources   Sources
Vers Mode Uptime    Expires   Timer      Timer      Forwarded Blocked
---- ---- --------- --------- ---------- ---------- --------- --------
3    INC  8m 10s    2m 21s                          1

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
```

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
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 igmp interface groups

`show ip igmp [interface {vlan <VLAN-ID>} [groups]]`

Description

Shows IGMP group information for a specific interface or VLAN interface.

Parameter	Description
`vlan <VLAN-ID>`	Specifies a VLAN. Values: 1-4094.
`<GROUP-IP>`	Specifies the IP address of the group. Format: A.B.C.D

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

                                V1         V2         Sources    Sources
Vers Mode Uptime     Expires    Timer      Timer      Forwarded  Blocked
---- ---- --------- ---------- ---------- ---------- ---------- --------
3    INC  4m 40s     3m 51s                           1

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

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded 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
```

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	Operator (>) or Manager (#)	Operators 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 { vlan <VLAN-ID>} statistics`

Description

Shows IGMP statistics for a specific interface or VLAN interface, including groups joined.

Parameter	Description
`vlan <VLAN-ID>`	Specifies a VLAN. Values: 1-4094.

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
```

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
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 igmp static-groups

```
show ip igmp static-groups [all-vrfs]
```

Description

Shows IGMP static groups, or shows information by VRF.

Parameter	Description
`all-vrfs`	Specify **all-vrfs** to show information for all VRFs.

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   :default
Interface Name   Group Address
---------------- -----------------
vlan10            238.1.1.1
```

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	Operator (>) or Manager (#)	Operators 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 [all-vrfs]
```

Description

Shows IGMP statistics, including groups joined, or shows statistics by VRF.

Parameter	Description
`all-vrfs`	Specify **all-vrfs** to show information for all VRFs.

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       : default

Number of Include Groups       :   1
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   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	Operator (>) or Manager (#)	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 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 proccessed. 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 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 **vlan-shared.**
`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 filter unknown mcast

```
ip igmp snooping filter-unknown-mcast
no ip igmp snooping filter-unknown-mcast
```

Description

Enables the avoidance of initial flooding of unknown multicast traffic on IGMP-snooping-enabled VLANs.

The no form of this command returns to the default behavior of initial flooding of unknown multicast traffic.

Usage

In the default behavior, the unknown multicast traffic is flooded until the IP Multicast Flow programming is done on the hardware. This is known as initial flooding of unknown multicast. Use this command to filter unknown multicast instead of flooding.

Initial flooding of multicast traffic is observed for a few seconds after the device comes up from a reboot. This issue is only seen when the multicast source connected device is rebooted. Once the device is up after a reboot, it takes a few seconds for the CPU Rx rule to be programmed during the timeframe that the initial flooding is observed. This is an expected behavior.

Example

Configure the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# ip igmp snooping filter-unknown-mcast
```

Removing the configuration of the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# no ip igmp snooping filter-unknown-mcast
```

Command History

Release	Modification
10.14	Command introduced on the 4100i, 6000, and 6100 switch series.

Command Information

Platforms	Command context	Authority
6000 6100	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).
`blocked vlan <VLAN-LIST>`	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

Parameter	Description
	(10, 20, 30, 40), dashes (10-40), or both (10-40,60).
`fastleave vlan <VLAN-LIST>`	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. 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. 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).
`forced-fastleave vlan <VLAN-LIST>`	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. 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). This command is available in **config-if** mode.
`forward vlan <VLAN-LIST>`	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). This command is available in **config-if** mode.
`no ...`	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
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip igmp snooping preprogram-starg-flow

```
ip igmp snooping preprogram-starg-flow {enable | disable}
```

Description

Configures preprogramming of the starg flow feature on the IGMP snooping enabled VLAN.

Parameter	Description
`enable`	Enables preprogramming starg flows on the VLAN.
`disable`	Disables preprogramming starg flows on the VLAN.

Usage

When this feature is enabled, a summarized multicast bridge entry is programmed into the hardware table when an IGMPv2 or IGMPv3 join is received on the IGMP snooping enabled VLAN. This enables multicast flow to be programmed in the hardware before the data packet arrives for a multicast flow. If an unknown packet is received for a multicast flow, having this feature enabled triggers programming of starg entry in the hardware on selected platforms, which is helpful in optimizing hardware resource utilization and PIM registration in deployments where a L2 device is connected along the PIM registration path.

This feature is currently supported for IGMPv2 and IGMPv3 joins, so IGMPv3 joins that are sent for a specific source are treated as IGMPv2 joins and summarized entry is programmed in the corresponding hardware.

Preprogramming of starg flows is supported only on the IGMP snooping enabled VLANs. If IGMP snooping is disabled on a VLAN, this feature is auto-disabled.

This feature is currently supported for IGMPv2 and IGMPv3 joins, as a result, summarized multicast flow is programmed in advance when an IGMPv2 join or IGMPv3 join for a specific group is received. For IGMPv3 deployments, traffic from all sources for a specific multicast group is sent to all clients, regardless of whether they send IGMPv2 or IGMPv3 joins for this group. Keeping this feature disabled is recommended on VLANs where traffic from the specific source is only expected for the IGMPv3 clients.

On the 4100i, 6000, and 6100 switch series, a single starg entry is programmed in advance for each join received and data driven programming of SG entries occurs when the traffic is received from a specific source for this group. As a result, the starg entry is used to forward the initial traffic and the SG entries programmed in the multicast forwarding table are used to forward subsequent traffic to all of the clients (that have sent either IGMPv2 joins or IGMPv3 joins) for all of the active joins in the feature enabled VLANs.

When an unknown multicast packet is received on a VLAN where this feature is enabled, it triggers programming of a starg entry in the hardware instead of the SG.

It is highly recommended to not enable this feature on devices where PIM or L3 multicast routing is enabled as it can lead to issues like permanent traffic loss.

Configuring this feature on devices where there are multiple sources sending traffic for the same group address is recommended.

This feature is mutually exclusive with the IGMP snooping static group feature.

Example

Enable preprogramming multicast starg flows:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping preprogram-starg flow enable
```

Disable preprogramming multicast starg flows:

```
switch(config)# vlan 2
switch(config-vlan-2)# ip igmp snooping preprogram-starg flow 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
6000 6100	config-vlan	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 (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 configurethe ACL on a particular interface.

Disabling and enabling IGMP snooping on a VLAN causes IGMP querier re-election.

Parameter	Description
`access-list`	Associates an ACL with the IGMP.
`enable|disable`	Enables or disables IGMP snooping on the VLAN. By default, IGMP snooping is disabled.
`no ...`	Negates any configured parameter.
`static-group` *`<MULTICAST-IP-ADDRESS>`*	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
`version <2-3>`	Configures the IGMP snooping version on the VLAN. Select **2** for IGMPv2 (RFC2236). Select **3** 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

Enable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping enable
```

Disable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping disable
```

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
10.07 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>}]
```

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 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 **vlan <vlan-id>** 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 **client details** parameter to display IGMP snooping client details.
`port <IF-NAME>`	Shows IGMP snooping group information for the interface name in **member**/**slot**/**port** format.
`vtep-peer <A.B.C.D>`	Shows IGMP snooping info for the specified VTEP.

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


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     3m 19s
200.1.1.1,200.1.1.2
                                                                 1/6/22
225.1.1.2              Filter    3    EXC  1m 2s     3m 19s
200.1.1.1,200.1.1.2
                                                                 1/6/22
226.1.1.1              Filter    3    EXC  1m 4s     3m 16s     200.1.1.3
226.1.1.2              Filter    3    EXC  1m 4s     3m 16s     200.1.1.3
```

Showing IGMP snooping packet exceptions:

```
switch#  show ip igmp snooping packet-exceptions
List of L2 Multicast Bridge entries for which data packets are hitting CPU

VRF: default
```

```
Vlan   Group Address          Source-Address          Packet Count   Last Seen
Time
----   --------------------   ---------------------   ------------   -------------
------------
10     232.2.2.2/32           100.100.1.10/32         19             00h:02m:03s
10     232.2.2.3/32           100.100.1.10/32         42             01h:01m:59s
10     232.2.2.3/32           100.100.1.11/32         32             28d:10h:01m
20     232.2.2.2/32           50.1.1.10/32            31             01m:02w:01d
20     233.2.2.2/32           50.1.1.10/32            38
0001y:02m:02w:05d
```

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

Command History

Release	Modification
10.13	Programming starg flow is now supported.
10.10	The **packet-exceptions** 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.

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.

Ccontinue (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
6100	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: **member/slot/port** or **member/slot/port-member/slot/port** 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.

energy-efficient-ethernet

`energy-efficient-ethernet`

Description

Enables auto-negotiation of Energy-Efficient Ethernet (EEE) on an interface. EEE Negotiation is established only on auto-link negotiation with supported link partners.

Examples

Configuring an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# energy-efficient-ethernet
```

Disabling Energy Efficient Ethernet on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no energy-efficient-ethernet
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

flow-control

```
flow-control rxtx
no flow-control rxtx
```

Description

Command **flow-control** enables negotiation of IEEE 802.3x link-level flow control on the current interface. The switch advertises link-level flow control support to the link partner. The final configuration is determined based on the capabilities of both partners.

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
`rxtx`	Enables the ability to honor received and to transmit IEEE 802.3x LLFC pause frames to the remote device.

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.
- Lossless flow control will only operate correctly when both the ingress and egress interfaces have flow control enabled.

Examples

Enabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control txrx
```

Disabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control txrx
```

hat 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.

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: **member/slot/port**.

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 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 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>
no ip address <IP-ADDR>/<MASK>
```

Description

Sets an IP/IPv6 address on the interface VLAN.

The **no** form of this command removes the IP/IPv6 address from the 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. 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 128.

Examples

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-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-vlan)# ip mtu 576
```

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-vlan`	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 **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**.
<MASK>	Specifies the number of bits in the address mask in CIDR format (**x**), where **x** 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.

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.

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 **access** persona type.
`uplink`	Selects the **uplink** persona type.
`custom <PERSONA-NAME>`	Selects the **custom** 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.
`attach`	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
10.10	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.

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 | vlan ] [<ID>] [brief]
show interface lag [<LAG-ID>] [extended [non-zero] | [human-readable]]
show interface lag [<LAG-ID>] monitor [human-readable]
```

Description

Shows active configurations and operational status information for interfaces.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.

Parameter	Description
`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.
`VLAN`	Shows VLAN interface information.
`<LAG-ID>`	Specifies the LAG number. Range: 1-256
`<VLAN-ID>`	Specifies the VLAN ID. Range: 1-4094

Examples

Showing information when interface 1/1/1 is configured:

```
MDI mode: MDIX
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: all
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
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 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 currently linked with energy-efficient-ethernet negotiated:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...
Energy-Efficient Ethernet is enabled and active
```

Showing information when the interface is configured with EEE and the EEE has auto-negotiated:

```
switch(config-if)# show interface 1/1/1 physical
------------------------------------------------------------------------------
------------------------------------------------------------
                            Link    Admin         Speed           Flow-Control
     EEE       PoE Power                          Port
Port        Type           Status   Config   Status | Config    Status | Config
Status | Config  (Watts)    State Information  Description
------------------------------------------------------------------------------
------------------------------------------------------------
1/1/1       1GbT           up       up       1G       auto      off      off
on       on       --        10M/100M/1G        --
```

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
                              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:

```
------------------------------------------------------------
                              Physical    Link         Last
Port           Type           Link State  Transitions  Change
------------------------------------------------------------
loopback1      --             up          --           --
```

Showing interface 1/1/2-1/1/3 link-status:

```
-------------------------------------------------------------
                              Physical    Link         Last
Port          Type            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           --
```

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 `monitor` parameter.
10.10	Added `human-readable` 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]`

Description

Shows diagnostics information and alarm/warning flags for the optical transceivers (SFP, SFP+). 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: **member/slot/port**.
`detail`	Show detailed information.

Example

```
switch# show interface dom
-------------------------------------------------------------------------------
Port    Type      Channel  Temperature Voltage  Tx Bias  Rx Power      Tx Power
                           (Celsius)   (Volts)  (mA)     (mW/dBm)      (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 energy-efficient ethernet

`show interface [<IFNAME>|<IFRANGE>] energy-efficient-ethernet`

Description

Displays Energy-Efficient Ethernet information for the interface.

Parameter	Description
<IFNAME>	Specifies the name of an interface on the switch. Use the format **member/slot/port** (for example, **1/1/1**).
<IFRANGE>	Specifies the port identifier range of an interface on the switch. Use the format **member/slot/port** (for example, **1/1/1**).

Example

The following example shows when the interfaces are Energy-Efficient Ethernet capable.

```
switch# show interface energy-efficient-ethernet
-------------------------------------------------------------------
Port     Enabled    Negotiated   Speed       TX Wake     RX Wake
                                 (MB/s)      Time(us)    Time (us)
-------------------------------------------------------------------
1/1/1    no         no           --          --          --
1/1/2    yes        yes          100         36          36
1/1/3    yes        yes          1000        17          17
1/1/4    no         no           --          --          --
1/1/5    yes        no           1000        --          --
```

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
6000 6100	`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 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
<IFNNAME>|<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                                 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                 pending           1234
             status: none
 1/1/12      config: pfc rxtx-1,2                 pending              0
             status: none
 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 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]
```

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.

Parameter	Description
`LAG`	Shows LAG interface information.
<LAG-ID>	Specifies the LAG number. Range: 1-256
`monitor`	Continuously monitor interface statistics.
`human-readable`	Shows statistics rounded to the nearest power of 1000, for example, 1K, 345M, 2G.
`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 Pa
-------------------------------------------------------------------------------------------------------------------------------------------------------
1/1/1                    2727136         1975         0     17796         195         0            82         1788           96           54         0
1/1/10                         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
1/1/12                         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
1/1/31      - lag2          2360           25        50   2732119        2040         0             0            0          178         1839         0
1/1/32      - lag2             0            0         0     11373          93         0             0            0            0           51         0
vlan1                          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   Runs   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 `moitor` parameter.
10.10	Added `human-readable` 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]
```

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 **member/slot/port** (for example, **1/3/1**).
`detail`	Show detailed information for the interfaces.
`threshold-violations`	Show threshold violations for transceivers.

Example

Showing summary transceiver information with identification of unsupported transceivers:

```
switch(config)# show interface transceiver
-------------------------------------------------------------------
Port      Type           Product      Serial          Part
                         Number       Number          Number
-------------------------------------------------------------------
1/1/15    SFP+SR         J9150D       xxxxxxxxxx      1990-4634
1/1/16    SFP+SR         J9150D       xxxxxxxxxx      1990-4634
```

Showing detailed transceiver information:

```
switch(config)# show interface transceiver detail
Transceiver in 1/1/15
 Interface Name      : 1/1/15
 Type                : SFP+SR
 Connector Type      : LC
 Wavelength          : 850nm
 Transfer Distance   : 0.00km (SMF), 20m (OM1), 80m (OM2), 300m (OM3)
 Diagnostic Support  : DOM
 Product Number      : J9150D
 Serial Number       : xxxxxxxxxx
 Part Number         : 1990-4634

Status
 Temperature : 30.38C
 Voltage     : 3.26V
 Tx Bias     : 5.54mA
 Rx Power    : 0.56mW, -2.52dBm
 Tx Power    : 0.62mW, -2.08dBm
 Recent Alarms:
 Recent Errors:

Transceiver in 1/1/16
 Interface Name      : 1/1/16
 Type                : SFP+SR
 Connector Type      : LC
 Wavelength          : 850nm
 Transfer Distance   : 0.00km (SMF), 20m (OM1), 80m (OM2), 300m (OM3)
 Diagnostic Support  : DOM
 Product Number      : J9150D
 Serial Number       : xxxxxxxxxx
 Part Number         : 1990-4634

Status
```

```
 Temperature : 30.62C
 Voltage     : 3.28V
 Tx Bias     : 5.64mA
 Rx Power    : 0.61mW, -2.15dBm
 Tx Power    : 0.59mW, -2.29dBm

Recent Alarms:
Recent Errors:
```

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#  Recent Threshold Violations
-------------------------------------------------------------------
1/1/15    SFP+SR                   none
1/1/16    SFP+SR                   none

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.

show interface utilization

`show interface [<IFNNAME>|<IFRANGE>] utilization [non-zero]`

Description

Displays physical port throughput and utilization.

Parameter	Description
<IFNAME>	Specifies an interface name.
<IFRANGE>	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>
```

Description

Shows status and configuration information for an IPv4 interface.

Parameter	Description
<INTERFACE-ID>	Specifies the name of an interface. Format: **member/slot/port**.

Example

```
switch# show ip interface vlan1
Interface vlan1 is up
Admin state is up
Hardware: Ethernet, MAC Address: f8:60:f0:c9:11:60
IP MTU 1500
IPv4 address 10.120.3.8/26
```

```
switch# show interface <intfid>.id
Interface 1/1/14.1 is up
Admin state is up
IP MTU 1500
Description:
Hardware: Ethernet, MAC Address: b8:6a:97:22:2f:42
Encapsulation dot1q ID: 20
IPv4 address 30.0.0.1/24
L3 Counters: Rx Disabled, Tx Disable
```

```
switch# show interface lag2.1
Interface lag2.1 is up
Admin state is up
IP MTU 1500
Description:
Hardware: Ethernet, MAC Address: b8:6a:97:22:2f:42
Encapsulation dot1q ID: 30
L3 Counters: Rx Disabled, Tx 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
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>]`

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 **all** option shows the global setting that applies to all protocols that do not have an address set.

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        Src-Interface       Src-IP                    VRF
-------------------------------------------------------------------
all             vlan2               2.2.2.2             default
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 (#)	Administrators or local user group members with execution rights for this command.

show ipv6 interface

`show ipv6 interface <INTERFACE-ID>`

Description

Shows status and configuration information for an IPv6 interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface ID. Format: **member/slot/port**.

Examples

```
switch# show ipv6 interface vlan2
Interface vlan2 is up
  Admin state is up
    IPv6 address:
      2001::1/64 [VALID]
    IPv6 link-local address: fe80::883a:3080:247:c1c0/64 [VALID]
    IPv6 Forwarding feature: enabled
    IPv6 multicast groups locally joined:
      ff02::1  ff02::1:ff00:1  ff02::1:ff47:c1c0  ff02::1:ff00:0
      ff02::2
    IPv6 MTU 1500
    IPv6 unicast reverse path forwarding: none
    IPv6 load sharing: none
switch#
```

```
switch# show ipv6 interface <intfid>.id
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 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 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
10.07 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.

```
switch# show ipv6 interface vlan2
Interface vlan2 is up
  Admin state is up
    IPv6 address:
      2001::1/64 [VALID]
    IPv6 link-local address: fe80::883a:3080:247:c1c0/64 [VALID]
    IPv6 Forwarding feature: enabled
```

```
    IPv6 multicast groups locally joined:
      ff02::1  ff02::1:ff00:1  ff02::1:ff47:c1c0  ff02::1:ff00:0
      ff02::2
    IPv6 MTU 1500
    IPv6 unicast reverse path forwarding: none
    IPv6 load sharing: none
switch#
```

show ipv6 source-interface

`show ipv6 source-interface {sflow | tftp | radius | tacacs | all} [vrf <VRF-NAME>]`

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 **all** 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.

Examples

Showing single source IP 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 IP address configuration settings for all protocols:

```
switch# show ipv6 source-interface all

Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP         VRF
------------------------------------------------------------------
 all             vlan2               2001::1       default

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 (#)	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.

speed

```
speed {<SPEED> | <SPEED-DUPLEX> | auto [<SPEED>] }
no speed
```

Description

Configures the link speed, duplex, and auto-negotiation settings for an interface.

The no form of this command removes the configurations and returns to the defaults.

Parameter	Description
`Speed`	Configures interface speed, duplex, and auto-negotiation.
`10-full`	10 Mbps, full duplex, no auto-negotiation
`10-half`	10 Mbps, half duplex, no auto-negotiation
`100-full`	100 Mbps, full duplex, no auto-negotiation
`100-half`	100 Mbps, half duplex, no auto-negotiation
`1000-full`	1000 Mbps, full duplex, no auto-negotiation
`10g`	10 Gbps, full duplex, no auto-negotiation
`25g`	25 Gbps, full duplex, no auto-negotiation
`40g`	40 Gbps, full duplex, no auto-negotiation
`50g`	50 Gbps, full duplex, no auto-negotiation
`100g`	100 Gbps, full duplex, no auto-negotiation
`200g`	200 Gbps, full duplex, no auto-negotiation **NOTE:** Not applicable for override.
`400g`	400 Gbps, full duplex, no auto-negotiation **NOTE:** Not applicable for override.
`auto`	Auto-negotiate speed and duplex. More than one speed can be set at a time.
`10m`	Allow interface to link at 10 Mbps.
`100m`	Allow interface to link at 100 Mbps.
`1g`	Allow interface to link at 1 Gbps.
`2.5g`	Allow interface to link at 2.5 Gbps.
`5g`	Allow interface to link at 5 Gbps.
`10g`	Allow interface to link at 10 Gbps.
`25g`	Allow interface to link at 25 Gbps.

Parameter	Description
`40g`	Allow interface to link at 40 Gbps.
`50g`	Allow interface to link at 50 Gbps.
`100g`	Allow interface to link at 100 Gbps.
`200g`	Allow interface to link at 200 Gbps.
`400g`	Allow interface to link at 400 Gbps.

Usage

The following options can be configured for an interface. The option available is based on the interface type.

`speed <SPEED-DUPLEX>`

Uses a fixed speed and duplex mode with no auto-negotiation. Half-duplex is only supported for 10 Mbps and 100 Mbps link speeds.

`speed <SPEED>`

Uses a fixed speed with no auto-negotiation. If the currently installed transceiver does not support the speed, the setting is ignored and the port will use the highest speed that is supported.

`speed auto`

Uses auto-negotiation and offers all speeds supported by the port and transceiver. This is the default. If the link technology does not support auto-negotiation this setting is ignored, and the port uses the highest possible fixed speed.

`speed auto <SPEED>`

Uses auto-negotiation and offers the specified speeds only. For ports that support pluggable transceivers, only speeds supported by the transceiver are offered and other speeds are ignored. If the link technology does not support auto-negotiation, this setting is ignored and the port uses the highest possible fixed speed.

Examples

Configuring an interface to operate at a fixed speed of 1000 Mbps with full duplex and no auto-negotiation:

```
switch(config)# interface 1/1/1

switch(config-if)# speed 1000-full
```

Configuring an interface to operate at a fixed speed of 10 Gbps with no auto-negotiation:

```
switch(config)# interface 1/1

switch(config-if)# speed 10g
```

Configuring an interface to auto-negotiate and advertise only 1 Gbps and 2.5 Gbps speeds:

```
switch(config)# interface 1/1/1
switch(config-if)# speed auto 1g 2.5g
```

Configuring an interface to override the detected transceiver speed and use the configured speed if the installed transceiver does not support auto-negotiation:

```
switch(config)# interface 1/1/1
switch(config-if)#speed auto 50g override
```

Configuring an interface to use default settings for speed, duplex, and auto-negotiation:

```
switch(config)# interface 1/1/1
switch(config-if)#no speed
```

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

Command History

Release	Modification
10.09.0001	Speeds not supported by hardware hidden by CLI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

client track ip

```
client track ip
```

Description

Enables client IP address tracking on the switch. The default is disabled on global and VLAN levels.

Admin users can enable client IP address tracking at the VLAN level.

Tracking enabling will take effect only if the client IP address tracking is enabled at system and VLAN level.

The **no** form of the command disables client IP address tracking. If tracking is disabled at switch level, it will be stopped even if it is enabled at VLAN or port level.

Example

Enable client IP address tracking at switch level:

```
switch(config)# client track ip
```

Enable client IP address tracking on VLAN 100:

```
switch(config)# vlan 100
switch(config-vlan-100)# client track ip
```

Enable client IP address tracking on VLANs 10 to 100:

```
switch(config)# vlan 10-100
switch(config-vlan-<10-100>)# client track 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
6000 6100	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.

client track ip { enable | disable | auto }

```
client track ip { enable | disable | auto }
```

Description

Enables client IP address tracking on the specified set of interfaces. Tracking will take effect only if client IP address tracking is enabled at both the system level and for the VLAN to which the port belongs. Default: auto.

The **no** form of the command disables client IP address tracking on the specified set of interfaces.

Parameter	Description
enable	Specifies that all client IP addresses will be tracked in the port.
disable	Specifies that client IP addresses will not be tracked in the port.
auto	Specifies the following: For LLDP devices: Only the specified client IP address will be tracked in the port and other client IP addresses will not be tracked. For non-LLDP devices: All client IP addresses will be tracked in the port.

Example

Enable client IP address tracking on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# client track ip enable
```

Enable client IP address tracking 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>)# client track 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
6000 6100	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.

client track ip client-limit

```
client track ip client-limit <CLIENT-LIMIT>
```

Description

Configures the maximum number of clients to be tracked on the specified set of interfaces.

For the 6000 and 6100 Switch Series the **no** form of the command resets the client limit to the default value of 128.

Parameter	Description
CLIENT-LIMIT	Specifies the maximum number of clients tracked on a port. Required. For the 6000 and 6100 Switch Series, Range: 1-128. Default: 128.

Example

Configure the maximum number of clients to be tracked on interface 1/1/5:

```
switch(config)# interface 1/1/5
switch(config-if)# client track ip client-limit 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
6000 6100	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.

client track ip update-interval

```
client track ip update-interval <INTERVAL>
```

Description

Configures how often client IP addresses are updated.

The **no** form of the command resets the update interval to the default of 1800 seconds.

Parameter	Description
INTERVAL	Specifies the update interval in seconds. Required. Range: 60-28000. Default: 1800.

Example

Configure the update interval for an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# client track ip update-interval 600
```

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	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.

client track ip update-method probe

```
client track ip update-method probe
```

Description

Enables probing the client to update the IP address.

The probe is sent to all clients on the tracking list that have an IP address in the following scenarios:

1. IP packets are not received from the clients during the IP address update cycle.
2. There is no IP packet from a learned IP address. In this case, a probe will be sent for the IP address to confirm if it is still owned by that client.

The **no** form of the command disables probing.

Example

Disable probing to update the client IP address:

```
switch(config)# no client track ip update-method probe
```

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`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 capacities

```
show capacities
```

Description

Shows the capacities configured on the switch.

Example

```
switch# show capacities

System Capacities:
Capacities Name                                                                  Value
--------------------------------------------------------------------------------------
Maximum number of Access Control Entries configurable in a system              14336
Maximum number of Access Control Lists configurable in a system                 1024
Maximum number of class entries configurable in a system                        1024
Maximum number of classes configurable in a system                               512
Maximum number of entries in an Access Control List                             1024
Maximum number of entries in a class                                            1024
Maximum number of entries in a policy                                           1024
Maximum number of classifier policies configurable in a system                   512
Maximum number of policy entries configurable in a system                       1024
Maximum number of clients supported for tracking the IP address in the system   128

switch# show capacities client-track-ip-client-limit

System Capacities: Filter Client Track IP Client Limit
Capacities Name
Value
--------------------------------------------------------------------------------
-
Maximum number of clients supported for tracking the IP address in the system
```

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>)	Administrators or local user group members with execution rights for this command.

show client ip { count | port | vlan }

```
show client ip { count | port | vlan }
```

Description

Shows number of client IP addresses or information about client IP addresses tracked on ports and VLANs.

Parameter	Description
count	Displays number of clients tracked.
port	Displays client IP addresses tracked on the ports.
vlan	Displays client IP addresses tracked on the VLANs.

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>)	Administrators or local user group members with execution rights for this command.

ipv4 source-binding

```
ipv4 source-binding <VLAN-ID> <IPV4-ADDR> <MAC-ADDR> <IFNAME>
no ipv4 source-binding <VLAN-ID> <IPV4-ADDR> <MAC-ADDR> <IFNAME>
```

Description

Adds static IPv4 client source binding information to the switch IP binding database. Although DHCPv4 snooping is often used to dynamically populate the binding database, this command is available for manually adding entries to the switch IP binding database.

Statically configured IP binding information supersedes any dynamically collected binding information for the same client.

The no form of this command removes the specified binding that was statically configured with the **ipv4 source-binding** command. The no form has no effect on bindings that were dynamically configured with DHCPv4 snooping.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPV4-ADDR>	Specifies the client IPv4 unicast address.
<MAC-ADDR>	Specifies the client MAC address.
<IFNAME>	Specifies the interface on which the client is connected.

Examples

Adding a static IPv4 binding:

```
switch(config)# ipv4 source-binding 1 10.2.1.4 00:50:56:96:e4:cf 1/1/1
```

Removing a IPv4 binding:

```
switch(config)# no ipv4 source-binding 1 10.2.1.4 00:50:56:96:e4:cf 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
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

ipv4 source-lockdown

```
ipv4 source-lockdown
no ipv4 source-lockdown
```

Description

Enables IPv4 source lockdown for all VLANs on the selected interface (port).

The no form of this command disables IPv4 source lockdown for the selected interface (port).

This configuration will disable flow tracking statistics collection.

Examples

Enabling IPv4 source lockdown on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv4 source-lockdown
```

Enabling IPv4 source lockdown on interface lag112:

```
switch(config)# interface lag112
switch(config-if)# ipv4 source-lockdown
```

Disabling IPv4 source lockdown on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv4 source-lockdown
```

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	Added information related to role based IPFIX.
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

ipv4 source-lockdown hardware retry

`ipv4 source-lockdown hardware retry <VLAN-ID> <IPV4-ADDR>`

Description

Retries the IPv4 source lockdown hardware programming for a client identified by VLAN and IPv4 address.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPV4-ADDR>	Specifies the client IPv4 unicast address.

Example

Configure IPv4 source lockdown hardware retry for the client on VLAN 10.

```
switch(config)# ipv4 source-lockdown hardware retry 10 1.1.2.1
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	config	Administrators or local user group members with execution rights for this command.

show ipv4 source-binding

```
show ipv4 source-binding
```

Description

Shows all IPv4 static source binding information irrespective of source lockdown configuration..

Examples

Showing all IPv4 source binding information:

```
switch# show ipv4 source-binding

  PORT            VLAN       MAC-ADDRESS        HW-STATUS  FROM      IPv4-ADDRESS
  --------------  ---------  -----------------  ---------  --------  -------------
  1/1/1           2          aa:bb:cc:dd:ee:ff  Yes        static    1.2.3.4
  1/1/2           12         aa:ab:cc:dd:ee:ff  Yes        static    10.20.30.40
```

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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv4 source-lockdown

```
show ipv4 source-lockdown [binding [interface <IFNAME> | ip <IPV4-ADDR> | mac <MAC-ADDR>
| vlan <VLAN-ID>] | interface <IFNAME>]
```

Description

Shows summary or detailed IPv4 source lockdown information. When entered without parameters, summary status information for all interfaces (ports) in the binding database is shown.

Parameter	Description
`binding`	Specifies that detailed lockdown binding record information is to be displayed. The binding database record can be identified by any one of **interface** (port), **ip**, **mac**, or **vlan**.
`interface <IFNAME>`	Specifies the client interface (port). When entered without the **binding** parameter, the summary status information is displayed for the specified interface.
`ip <IPV4-ADDR>`	Specifies the client IPv4 unicast address.
`mac <MAC-ADDR>`	Specifies the client MAC address.
`vlan <VLAN-ID>`	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.

Examples

Showing the summary status information for all interfaces in the binding database:

```
switch# show ipv4 source-lockdown

  INTERFACE  LOCKDOWN  HW-STATUS
  ---------  --------  ---------
  1/1/1      Yes       Yes
  1/1/2      Yes       No
  lag112     Yes       Yes
```

Showing the summary status information for the specified interface in the binding database:

```
switch# show ipv4 source-lockdown interface 1/1/2

  INTERFACE  LOCKDOWN  HW-STATUS
  ---------  --------  ---------
  1/1/2      Yes        No
```

Showing the detailed binding record and related information for all interfaces in the binding database:

```
switch# show ipv4 source-lockdown binding

 Interface Name        : 1/1/1
 VLAN Id               : 2000
 MAC Address           : 00:50:56:96:e4:cf
 IP Address            : 192.168.142.113
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --

 Interface Name        : 1/1/2
 VLAN Id               : 100
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 120.168.43.52
 Time Remaining        : 115 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
```

```
 Hardware Error Reason : Resource unavailable

 Interface Name        : lag112
 VLAN Id               : 12
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 120.168.76.182
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --

 Interface Name        : 1/1/1
 VLAN Id               : 2000
 MAC Address           : 00:50:56:96:e4:cf
 IP Address            : 192.168.142.113
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --

 Interface Name        : 1/1/2
 VLAN Id               : 100
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 120.168.43.52
 Time Remaining        : 115 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable

 Interface Name        : lag112
 VLAN Id               : 12
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 120.168.76.182
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface 1/1/2:

```
switch# show ipv4 source-lockdown binding interface 1/1/2

 Interface Name        : 1/1/2
 VLAN Id               : 100
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 120.168.43.52
 Time Remaining        : 115 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable

 Interface Name        : 1/1/2
 VLAN Id               : 100
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 120.168.43.52
 Time Remaining        : 115 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable
```

Showing the detailed binding record and related information for interface lag112 (identified in this example command by the IP address):

```
switch# show ipv4 source-lockdown binding ip 120.168.76.182

 Interface Name        : lag112
 VLAN Id               : 12
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 120.168.76.182
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface 1/1/1 (identified in this example command by the MAC address):

```
switch# show ipv4 source-lockdown binding mac 00:50:56:96:e4:cf

 Interface Name        : 1/1/1
 VLAN Id               : 2000
 MAC Address           : 00:50:56:96:e4:cf
 IP Address            : 192.168.142.113
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface 1/1/2 (identified in this example command by the VLAN):

```
switch# show ipv4 source-lockdown binding vlan 100

 Interface Name        : 1/1/2
 VLAN Id               : 100
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 120.168.43.52
 Time Remaining        : 115 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable
```

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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 <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 vlan 2
switch(config-if-vlan)#  ipv6 address 3731:54:65fe:2::a7
```

Disabling a global unicast address:

```
switch(config)# interface vlan 2
switch(config-if-vlan)#  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-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 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 vlan 2
switch(config-if-vlan)# ipv6 address autoconfig
```

Disabling unicast autoconfiguring:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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	`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 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
<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 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**.
<MASK>	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 vlan 2
switch(config-if-vlan)# 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	`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 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
<CACHELIMIT>	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
`dad attempts` *<NUM-ATTEMPTS>*	Specifies the number of neighbor solicitations to send. Range: 0-15. Default: 1.

Examples

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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
<IPV6-ADDR>	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**.
`lifetime` *<TIME>*	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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
<TIME>	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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
<TIME>	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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 vlan 2
switch(config-if-vlan)# 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-vlan`	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		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 vlan 2
switch(config-if-vlan)# 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-vlan`	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
`suppress-ra [<SUPPRESS-OPTION>]`	Specifies suppressing RA transmissions. Entering suppress-ra without any options, suppresses all RA messages (default). Or you can enter one of the following options.
`dnssl`	Specifies suppressing DNSSL options in RA messages.
`mtu`	Specifies suppressing MTU options in RA messages.
`rdnss`	Specifies suppressing RDNSS options in RA messages.

Examples

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 nd suppress-ra mtu dnssl rdnss
switch(config-if-vlan)# 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	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

show ipv6 nd global traffic

```
show ipv6 nd global traffic
```

Description

Displays IPV6 Neighbor Discovery traffic details on a device.

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>]`

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.
`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.

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 vlan 2:

```
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>]
```

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.

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`

Description

Displays domain name information on all interfaces.

Examples

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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
```

Description

Displays DNS server information on all interfaces.

Examples

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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.

Chapter 39
IPv6 source lockdown commands

ipv6 source-binding

```
ipv6 source-binding <VLAN-ID> <IPV6-ADDR> <MAC-ADDR> <IFNAME>
no ipv6 source-binding <VLAN-ID> <IPV6-ADDR> <MAC-ADDR> <IFNAME>
```

Description

Adds static IPv6 client source binding information to the switch IPv6 binding database. Although DHCPv6 snooping is often used to dynamically populate the binding database, this command is available for manually adding entries to the switch IPv6 binding database.

Statically configured IPv6 binding information supersedes any dynamically collected binding information for the same client.

The no form of this command removes the specified binding that was statically configured with the **ipv6 source-binding** command. The no form has no effect on bindings that were dynamically configured with DHCPv6 snooping.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPV6-ADDR>	Specifies the client IPv6 address.
<MAC-ADDR>	Specifies the client MAC address.
<IFNAME>	Specifies the interface on which the client is connected.

Examples

Adding a static IPv6 binding:

```
switch(config)# ipv6 source-binding 2 2000::2 00:12:11:44:55:12 1/1/28
```

Removing a IPv6 binding:

```
switch(config)# no ipv6 source-binding 2 2000::2 00:12:11:44:55:12 1/1/28
```

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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

ipv6 source-lockdown

```
ipv6 source-lockdown
no ipv6 source-lockdown
```

Description

Enables IPv6 source lockdown for all VLANs on the selected interface (port).

The no form of this command disables IPv6 source lockdown for the selected interface (port).

This configuration will disable flow tracking statistics collection.

Examples

Enabling IPv6 source lockdown on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 source-lockdown
```

Enabling IPv6 source lockdown on interface lag112:

```
switch(config)# interface lag112
switch(config-if)# ipv6 source-lockdown
```

Disabling IPv6 source lockdown on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 source-lockdown
```

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	Added information related to role based IPFIX.
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 source-lockdown hardware retry

`ipv6 source-lockdown hardware retry <VLAN-ID> <IPV6-ADDR>`

Description

Retries the IPV6 source lockdown hardware programming for a client identified by VLAN and IPv6 address.

Parameter	Description
<VLAN-ID>	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.
<IPV6-ADDR>	Specifies the client IPv6 address.

Example

Configure IPv6 source lockdown hardware retry for the client on VLAN 1.

```
switch(config)# ipv6 source-lockdown hardware retry 1 2000::2
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show ipv6 source-binding

`show ipv6 source-binding`

Description

Shows all IPv6 static source binding information irrespective of source lockdown configuration.

Examples

Showing all IPv6 source binding information:

```
            switch# show ipv6 source-binding

PORT            VLAN       MAC-ADDRESS        HW-STATUS  FROM      IPv6-ADDRESS

--------------  ---------  -----------------  ---------  --------  -------------
1/1/1           1234        00:50:56:96:e4:cf  Yes/No     static    3000::1

1/1/1           1           00:50:56:96:04:4d  Yes/No     static    3000::2
1/1/24          1           00:01:01:00:00:01  Yes        static    1001::1
```

For more information on features that use this command, refer to the IP Services Guide for your switch model.

Command History

Release	Modification
10.10	Command enabled on 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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-lockdown

`show ipv6 source-lockdown [binding [interface <IFNAME> | ip <IPV6-ADDR> | mac <MAC-ADDR> | vlan <VLAN-ID>] | interface <IFNAME>]`

Description

Shows summary or detailed IPv6 source lockdown information. When entered without parameters, summary status information for all interfaces (ports) in the binding database is shown.

Parameter	Description
`binding`	Specifies that detailed lockdown binding record information is to be displayed. The binding database record can be identified by any one of **interface** (port), **ip**, **mac**, or **vlan**.
`interface <IFNAME>`	Specifies the client interface (port). When entered without the **binding** parameter, the summary status information is displayed for the specified interface.
`ip <IPV6-ADDR>`	Specifies the client IPv6 address.
`mac <MAC-ADDR>`	Specifies the client MAC address.
`vlan <VLAN-ID>`	Specifies the ID of an existing VLAN on which the client is connected. Range: 1 to 4094.

Examples

Showing the summary status information for all interfaces in the binding database:

```
switch# show ipv6 source-lockdown

  INTERFACE  LOCKDOWN  HW-STATUS
  ---------  --------  ---------
  1/1/1      Yes       Yes
  1/1/2      Yes       Yes
  lag112     Yes       Yes
```

Showing the summary status information for the specified interface in the binding database:

```
switch# show ipv6 source-lockdown interface 1/1/2

  INTERFACE  LOCKDOWN  HW-STATUS
  ---------  --------  ---------
  1/1/2      Yes       No
```

Showing the detailed binding record and related information for all interfaces in the binding database:

```
switch# show ipv6 source-lockdown binding

 Interface Name        : 1/1/1
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:e4:cf
 IP Address            : aaaa:bbbb:cccc:dddd:eeee:1234
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
```

```
 Time Remaining        : 3290 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable

 Interface Name        : lag112
 VLAN Id               : 151
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 1001::5
 Time Remaining        : 1200 seconds
 Lockdown Status       : No
 Hardware Status       : Yes
 Hardware Error Reason : --

 Interface Name        : 1/1/1
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:e4:cf
 IP Address            : aaaa:bbbb:cccc:dddd:eeee:1234
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
 Time Remaining        : 3290 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable

 Interface Name        : lag112
 VLAN Id               : 151
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 1001::5
 Time Remaining        : 1200 seconds
 Lockdown Status       : No
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface 1/1/2:

```
switch# show ipv6 source-lockdown binding interface 1/1/2

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
 Time Remaining        : 3290 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
 Hardware Error Reason : Resource unavailable

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
 Time Remaining        : 3290 seconds
 Lockdown Status       : Yes
 Hardware Status       : No
```

```
 Hardware Error Reason : Resource unavailable
```

Showing the detailed binding record and related information for interface 1/1/2 (identified in this example command by the IP address):

```
switch# show ipv6 source-lockdown binding ip 4000::1

 Interface Name        : 1/1/2
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:04:4d
 IP Address            : 4000::1
 Time Remaining        : 515 seconds
 Lockdown Status       : No
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface 1/1/1 (identified in this example command by the MAC address):

```
switch# show ipv6 source-lockdown binding mac 00:50:56:96:e4:cf

 Interface Name        : 1/1/1
 VLAN Id               : 1234
 MAC Address           : 00:50:56:96:e4:cf
 IP Address            : aaaa:bbbb:cccc:dddd:eeee:1234
 Time Remaining        : static
 Lockdown Status       : Yes
 Hardware Status       : Yes
 Hardware Error Reason : --
```

Showing the detailed binding record and related information for interface lag112 (identified in this example command by the VLAN):

```
switch# show ipv6 source-lockdown binding vlan 151

 Interface Name        : lag112
 VLAN Id               : 151
 MAC Address           : 00:50:56:96:d8:3d
 IP Address            : 1001::5
 Time Remaining        : 1200 seconds
 Lockdown Status       : No
 Hardware Status       : Yes
 Hardware Error Reason : --
```

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 4100i, 6000 and 6100 series switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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
`broadcast`	Advertisements are sent as broadcast packets to IP address 255.255.255.255.
`multicast`	Advertisements are sent as multicast packets to the multicast group with IP address 24.0.0.1. Default.

Examples

Enabling IRDP on interface vlan 2 with packet type set to the default value (multicast).

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp
```

Enabling IRDP on interface vlan 2 with packet type set to broadcast.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp broadcast
```

Disabling IRDP.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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-vlan`	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 VLAN interface 2 to 5000 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp holdtime 5000
```

Removing the the hold time for VLAN interface 2 to 5000 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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-vlan`	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 VLAN interface 2 to 30 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp maxadvertinterval 30
```

Removing the advertisement interval for VLAN interface 2 to 30 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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-vlan`	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 VLAN interface 2 to 25 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp minadvertinterval 25
```

Removing the minimum advertisement interval for VLAN interface 2 to 25 seconds:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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-vlan`	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 VLAN interface 2 to 25.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip irdp preference 25
```

Removing the IRDP preference level for VLAN interface 2 to 25.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# 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-vlan`	Administrators or local user group members with execution rights for this command.

show ip irdp

```
show ip irdp
```

Description

Displays IRDP configuration settings.

Example

```
switch# show ip irdp

ICMP Router Discovery Protocol

 Interface Status   Advertising Minimum  Maximum  Holdtime Preference
                    Address     Interval Interval
 --------- -------- ----------- -------- -------- -------- -----------
 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 Minimum  Maximum  Holdtime Preference
                          Address     Interval Interval
 --------------- -------- ----------- -------- -------- -------- -----------
 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.

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-PTog1)# 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-<NAME>`	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
<SCHEDULE-NAME>	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 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-<NAME>`	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
<JOB-NAME>	Specifies an existing job name. When omitted, information is shown for every job. Range: 1 to 64 characters (alphanumeric and "_" (underscore)).
<INSTANCE-ID>	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 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-*<NAME>* config-schedule-*<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.

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   : PTog1
```

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.

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 IDcorresponding 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        :
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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        :
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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        :
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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        :
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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        :
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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        :
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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 runnning-config keychain
```

Description

Shows the configurations for key chain protocol.

Example

```
switch# show running-config keychain
keychain ospf_keys
  key 1
    key-string ciphertext
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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
AQBapZ1OHiO9W3JwRqnjtLfbV73BPLS1S6TGVg+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.

downshift enable

```
downshift-enable
no downshift-enable
```

Description

Enables/disables automatic speed downshift on an interface that supports downshift, generally 1GBASE-T ports. When enabled, downshift allows an interface to link at a lower advertised speed when unable to establish a stable link at the maximum speed. Downshifting only applies to physical interfaces that are not members of a LAG and is only available when auto-negotiation is enabled. When only one speed is advertised, downshift will not be triggered.

Examples

```
switch(config-if)# interface 1/1/1
switch(config-if)# downshift-enable

Warning: this is a non-standard mode for use only when standards-based
auto-negotiation is not able to establish a stable link. Enabling this
may cause the port to link at a lower than expected speed and should
not be used on ports that are members of a LAG. Support calls may require
this feature to be disabled

Continue (y/n)?

switch(config-if)#
```

When automatic downshift is enabled:

```
switch(config-if)# show running-config interface
interface 1/1/1
    downshift-enable
```

Disabling automatic speed downshift:

```
switch(config-if)# interface 1/1/1
switch(config-if)# no downshift-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
6000 6100	`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 | vlan ] [<ID>] [brief]
show interface lag [<LAG-ID>] [extended [non-zero] | [human-readable]]
show interface lag [<LAG-ID>] monitor [human-readable]
```

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.
`VLAN`	Shows VLAN interface information.

Parameter	Description
<LAG-ID>	Specifies the LAG number. Range: 1-256
<VLAN-ID>	Specifies the VLAN ID. Range: 1-4094

Examples

Showing information when interface 1/1/1 is configured:

```
MDI mode: MDIX
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: all
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
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 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 currently linked with energy-efficient-ethernet negotiated:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...
Energy-Efficient Ethernet is enabled and active
```

Showing information when the interface is configured with EEE and the EEE has auto-negotiated:

```
switch(config-if)# show interface 1/1/1 physical
--------------------------------------------------------------------------------
--------------------------------------------------------
                            Link    Admin         Speed           Flow-Control
     EEE       PoE Power                        Port
Port        Type           Status   Config   Status | Config    Status | Config
Status | Config  (Watts)    State Information  Description
--------------------------------------------------------------------------------
--------------------------------------------------------
1/1/1       1GbT           up       up       1G       auto      off      off
on       on       --        10M/100M/1G        --
```

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
                              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:

```
------------------------------------------------------------
                              Physical    Link         Last
Port           Type           Link State  Transitions  Change
------------------------------------------------------------
loopback1      --             up          --           --
```

Showing interface 1/1/2-1/1/3 link-status:

```
------------------------------------------------------------
                              Physical    Link         Last
Port           Type           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           --
```

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 `monitor` parameter.
10.10	Added `human-readable` 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 downshift-enable

```
show interface [<IFNNAME>|<IFRANGE>] downshift-enable
```

Description

Displays speed downshift information, including the interface speed status and configuration.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.

Examples

Showing automatic downshift information:

```
switch(config-if)# show interface downshift-enable
-------------------------------------------------
              Downshift              Speed
Port      Enabled | Active    Status    | Config
-------------------------------------------------
1/1/1     yes       yes       100M-FDx    auto
1/1/2     yes       no        1G          auto
1/1/3     yes       no        100M-FDx    100M-FDx
1/1/4     no        no        --          auto
```

Showing automatic downshift information on per interface:

```
switch(config-if)# show interface 1/1/2 downshift-enable
-------------------------------------------------
              Downshift              Speed
Port      Enabled | Active    Status    | Config
-------------------------------------------------
1/1/2     yes       no        1G          auto
```

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
6000 6100	`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 interface

```
show running-config interface [<IFNNAME>|<IFRANGE>]
show running-config interface [lag | loopback | tunnel | vlan ] [<ID>]
```

Description

Displays active configurations of various switch interfaces.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
LAG	Specifies LAG interface information
LOOPBACK	Specifies loopback interface information.
TUNNEL	Specifies tunnel interface information.
VLAN	Specifies 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	Specifies the VXLAN interface information.
<VXLAN-ID>	Specifies the VXLAN interface identifier. Default: 1.

Examples

Showing 1/1/2 interface configuration:

```
switch(config-if)# show running-config interface 1/1/2

interface 1/1/2
   no shutdown
   description DC-23
   exit
```

Showing loopback interfaces configured:

```
switch(config-if)# show running-config interface loopback

interface loopback 1
    description lb interface 1
    exit
interface loopback 2
    description lb interface 2
    exit
```

Showing loopback interfaces not configured:

```
switch(config-if)# show running-config interface loopback

No loopback interfaces configured.
```

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
6000 6100	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.

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.

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
6000 6100	`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
<PORT-ID>	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
<PORT-PRIORITY>	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.

show interface

`show interfaces <LAG-NAME>`

Description

Displays information about a specific LAG.

Parameter	Description
<LAG-NAME>	Specifies a LAG name.

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 lacp aggregates

`show lacp aggregates [<LAG-NAME>]`

Description

Displays all LACP aggregate information configured for all LAGs, or for a specific LAG.

Parameter	Description
<LAG-NAME>	Optional: Specifies a lag name.

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                  : l3-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                  : l3-src-dst
Aggregate mode        : active


Aggregate-name        : lag2
Aggregated-interfaces : 1/1/48
Heartbeat rate        : slow
Hash                  : l2-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`

Description

Displays global LACP configuration.

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>]`

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.

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                               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                               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:

lacp fallback-staticcannot 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   Port    Port   State   System-id         System  Aggr Forwarding
       Name   Id      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                              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       Port  Port  State   System-ID         System Aggr Forwarding
        Name       Id    Pri                             Pri    Key  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            : l3-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                          : l3-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 lag

```
show running-config interface lag
```

Description

Displays the running configuration for interface lag.

Examples

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
```

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)# shutdown
```

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: 512 (6000 and 6100) 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 6000, 6100, and 6200 switch series:

```
switch(config)# interface lag 1
switch(config-lag-if)# no shutdown
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 6000, 6100, and 6200 switch series:

```
switch(config)# interface lag 1
switch(config-lag-if)# no shutdown
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.

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 eee

```
lldp dot3 eee
no lldp dot3 eee
```

Description

Sets the 802.3 TLVs for Energy-Efficient Ethernet (EEE) to be advertised. By default, advertisement of EEE TLVs is enabled.

The **no** form of this command disables advertisement of 802.3 TLVs.

Parameter	Description
`eee`	Specifies advertisement of 802.3 TLVs for EEE.

Examples

Enabling advertisement of the EEE TLVs:

```
switch(config-if)# lldp dot3 eee
```

Disabling advertisement of the EEE TLVs:

```
switch(config-if)# no lldp dot3 eee
```

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
6000 6100	`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 holdtime-multiplier

```
lldp holdtime-multiplier <multiplier>
no lldp holdtime-multiplier
```

Description

Sets the holdtime TTL multiplier value that is used to calculate the LLDP Time-to-Live value. Time-to-Live defines the length of time that neighbors consider LLDP information sent by this agent as valid. When Time-to-Live expires, the information is deleted by the neighbor. Time-to-live is calculated by multiplying holdtime by the value of **lldp timer**.

The **no** form of this command sets the holdtime TTL multiplier to its default value of 4.

Parameter	Description
<multiplier>	Specifies the TTL multiplier in the range of 2 to 10. Default: 4.

Formula

TTL = Holdtime-multiplier x lldp timer

where:

TTL = Time-to-Live

Holdtime-multiplier = Multiplying holdtime value

lldp timer = Message transmission interval

Examples

Setting the holdtime to 8 times of the value of lldp timer:

```
switch(config)# lldp holdtime-multiplier 8
```

Setting the holdtime to the default value of 4 times of the value of lldp timer:

```
switch(config)# no lldp holdtime-multiplier
```

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 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 SVI [interface VLAN <*vid*>]
- Base MAC address of the switch

The **no** form of this command removes the IPv4 management address of the switch.

Parameter	Description
<IPV4-ADDR>	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	`config`	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 SVI [interface VLAN <*vid*>]
- Base MAC address of the switch

The **no** form of this command removes the IPv6 management address of the switch.

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.

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.

The **no** form of this command disables support for the LLDP MED TLV.

Parameter	Description
`poe [priority-override]`	Specifies advertisement of power over Ethernet data link

Parameter	Description
	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.
`capability`	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.
`network-policy`	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	`config-if`	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.

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
```

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 (OUI) with the following Organization-specific TLVs:

- IEEE 802.1 (DOT1) (oui:0x00, 0x80, 0xc2)
- IEEE 802.3 (DOT3) (oui:0x00, 0x12, 0x0f)
- Aruba, a Hewlett Packard Enterprise Company (oui:0x88, 0x3a, 0x30)

Parameter	Description
`select-tlv <TLV-NAME>`	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. If layer 2, the IP address of the SVI. 3. 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
<TIME>	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 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.

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
```

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>]`

Description

Shows LLDP configuration settings for all interfaces or a specific interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**.

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
Med Priority Override         : Yes
Med Location Civic-addr       : US 1 4 ret 6 tyu 7 tiyuo
Med Location Elin-addr        : gher
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
10.07 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 local-device

```
show lldp local-device
```

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.

Example

Showing global LLDP information only:

```
switch# show lldp local-device

Global Data
===========

Chassis-ID             : 88:3a:30:47:c1:c0
System Name            : 6100
System Description     : Aruba JL679A  PL.10.06.0001-346-g56a12a8f4cf15
Management Address     : 88:3a:30:47:c1:c0
Capabilities Available : Bridge, Router
Capabilities Enabled   : Bridge, Router
TTL                    : 120
```

Showing all ports except **1/1/11** as administratively down:

```
switch# show lldp local-device

Global Data
===========

Chassis-ID             : 88:3a:30:47:c1:c0
System Name            : 6100
System Description     : Aruba JL679A  PL.10.06.0001-346-g56a12a8f4cf15
Management Address     : 11.11.11.11
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 : 11.11.11.11
Port VLAN ID      : 1
Parent Interface  : interface 1/1/11

switch#
```

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     : Aruba
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>]`

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**).

Examples

Showing LLDP information for all interfaces:

```
switch# show lldp neighbor-info

LLDP Neighbor Information
=========================
```

```
Total Neighbor Entries          : 1
Total Neighbor Entries Deleted  : 5
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 3

LOCAL-PORT  CHASSIS-ID         PORT-ID       PORT-DESC     TTL      SYS-NAME
--------------------------------------------------------------------------------
1/1/2       38:21:c7:5c:df:40  1/1/2         1/1/2         120      switch
1/1/3       f8:60:f0:c9:e0:a0  1/1/3         1/1/3         120      switch
```

Showing information for interface **1/1/3** when it has only one switch connected as a neighbor:

```
Aruba-6100-Switch2# show lldp neighbor-info 1/1/3

Port                           : 1/1/3
Neighbor Entries               : 1
Neighbor Entries Deleted       : 1
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 1
Neighbor Chassis-Name          : 6100
Neighbor Chassis-Description   : Aruba JL679A PL.10.06.0001
Neighbor Chassis-ID            : 88:3a:30:47:d1:c0
Neighbor Management-Address    : 88:3a:30:47:d1:c0
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/3
Neighbor Port-Desc             : 1/1/3
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-ned Advertised   : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighnor MAU Type              : 1000 BASETFD
```

Showing neighbor information for interface 1/3/2 when it has EEE enabled and successfully auto-negotiated:

```
switch# show lldp neighbor-info 1/3/2

Port                           : 1/3/2
Neighbor Entries               : 1
Neighbor Entries Deleted       : 1
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 1
Neighbor Chassis-Name          : BLDG01-F1-6300
Neighbor Chassis-Description   : Aruba JL668A  FL.10.07.0001BN
Neighbor Chassis-ID            : 88:3a:30:92:a5:c0
Neighbor Management-Address    : 10.6.9.15
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 Mac-Phy details
Neighbor Auto-neg Supported    : true
Neighbor Auto-Neg Enabled      : true
Neighbor Auto-Neg Advertised   : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type              : 1000 BASETFD

Neighbor EEE information       : DOT3
Neighbor TX Wake time          : 17 us
Neighbor RX Wake time          : 17 us
Neighbor Fallback time         : 17 us
Neighbor TX Echo time          : 17 us
Neighbor RX Echo time          : 17 us
```

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`

Description

Shows detailed LLDP neighbor information for all LLDP neighbor connected interfaces.

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    : Aruba ...
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 BASET_FD
Neighbor MAU type               : 1000 BASETFD

--------------------------------------------------------------------------------

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    : Aruba ...
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 BASET_FD
Neighbor MAU type               : 1000 BASETFD

--------------------------------------------------------------------------------

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   : Aruba ...
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 BASET_FD
Neighbor MAU type              : 1000 BASETFD

--------------------------------------------------------------------------------

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   : Aruba ...
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 BASET_FD
Neighbor MAU type              : 1000 BASETFD

--------------------------------------------------------------------------------

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   : Aruba ...
Neighbor Chassis-ID            : 38:11:17:1a:d5:00
Neighbor Management-Address    : 38:11:17:1a:d5:00
Chassis Cap
```

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

`show lldp statistics [<INTERFACE-ID>]`

Description

Shows global LLDP statistics or statistics for a specific interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**.

Example

Showing global statistics for all interfaces:

```
switch# show copp-policy statistics
switch# show lldp statistics
LLDP Global Statistics
================================================================================

Total Packets Transmitted            : 25
Total Packets Received               : 20
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           25             20             0              0
1/1/2           0              0              0              0
1/1/3           0              0              0              0
1/1/4           0              0              0              0
1/1/5           0              0              0              0
1/1/6           0              0              0              0
1/1/7           0              0              0              0
1/1/8           0              0              0              0
1/1/9           0              0              0              0
1/1/10          0              0              0              0
```

```
1/1/11          0                0                0                0
1/1/12          0                0                0                0
1/1/13          0                0                0                0
1/1/14          0                0                0                0
1/1/15          0                0                0                0
1/1/16          0                0                0                0
1/1/17          0                0                0                0
1/1/18          0                0                0                0
1/1/19          0                0                0                0
1/1/20          0                0                0                0
1/1/21          0                0                0                0
1/1/22          0                0                0                0
1/1/23          0                0                0                0
1/1/24          0                0                0                0
1/1/25          0                0                0                0
1/1/26          0                0                0                0
1/1/27          0                0                0                0
1/1/28          0                0                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 tlv

`show lldp tlv`

Description

Shows the LLDP TLVs that are configured for send and receive.

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> lockout-time <LOCKOUT-TIME>
no aaa authentication limit-login-attempts <ATTEMPTS> lockout-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 lockout using this command and also enable the console lockout 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 lockout 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 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 local login attempt failure limiting with a 20 second lockout being triggered upon the fourth consecutive login attempt failure.

```
switch(config)# aaa authentication limit-login-attempts 4 lockout-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

<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.

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 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

<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**) 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.
	`console`
	Selects the **console** connection type for configuration.
	`ssh`
	Selects the **ssh** connection type for configuration.

`local`	When used alone without `group` *<GROUP-LIST>*, 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` *<GROUP-LIST>*, 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` *<GROUP-LIST>*	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**

Parameter	Description
	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`

Description

Shows the accounting configuration per connection type (channel).

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
```

Description

Shows the authentication configuration per connection type (channel).

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
```

Description

Shows the authorization configuration per connection type (channel).

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
<USERNAME>	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 AAAAB3NzaC1yc2EAAAADAQABAAABAQDMtyMBmmAaF6r1zxf3DZNHSYVHBJhlbBlyAIqQ8DSHK
...
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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEqEFevZ0
...
l76V+D0svdCJ9Wo32zqI9OeAdTJw/eZYp5qknhNgS81HjAI6J/4/kAqdZAjbqQUiCAk= admin@switch

2. Key Type : RSA     Key size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDXQHrqV7+/GcMdOhr//IRjJkX7TQKupW89j80bL7xq8
...
j8qKuHWSN0/h/HxjzQJuYDVmZN5vG3DhpXbBZUlZNnchVod13QLCesqA3VLKN 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
<USERNAME>	Specifies the name of the user.
<PUBKEY>	Specifies the SSH client public key to be copied into the key list.
<KEYNUM>	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 AAAAE2VjZHNhLXNoYTIt
bmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEqEFevZ0l76V+D0svdCJ9Wo32zqI9OeAIdTJwT/eZYp50qkA
nhZNgS81HBjAI6QJ/4/kAyqdZ9oAjbiqQUiCAk= 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	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 threshold

```
logging threshold {audit-log | auth-log | commands-log |event-log | } <THRESHOLD%>
no logging threshold {audit-log | auth-log | commands-log | event-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.
`<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
```

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
```

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	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.

Parameter	Description
`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
```

Description

Shows the log rotate configuration.

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)# loop-protect
```

Enabling loop protection on LAG **25**:

```
switch# config
switch(config)# interface lag 25
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 2048 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.

Lower-capacity switches are not able to support this theoretical limit, value due to platform limitations regarding L2VNI and VTEP peers. (For example, 6200 Switch series allows up to 32 L2VNI and 16 VTEP peers.)

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>]`

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
<INTERFACE-NAME>	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**.

Loop protection on VXLAN interfaces is supported on AOS-CX 6200, 6300, 6400, 8360, 8325, 8400, 9300, 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.

Chapter 49
Loopback commands

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 4

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
<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 128.
secondary	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
<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.

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.

show interface loopback

`show interface loopback [brief | instance <ID>]`

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

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 **vxlan1**.
<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
```

Description

Shows MAC address table information.

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
```

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.
```

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>`

Description

Shows MAC address table information for a specific MAC address.

Parameter	Description
<MAC-ADDR>	Specifies the MAC address.

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>]
```

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.

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
```

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>]`

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.

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
```

Description

Shows MAC lockout table information.

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 case of MACs learnt on VXLAN tunnels or "port-access port-security" enabled ports, move scenario is handled by EVPN/port-access feature respectively and it performs the move by deleting the MAC from 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  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
```

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  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
```

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  10     1/1/27          1/1/28          2            Fri Sep 15
19:11:51 2023
```

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>`

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**.

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 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>
```

Description

Shows MAC addresses learned by or configured on the specified VLAN.

Parameter	Description
`vlan <VLAN-ID>`	Specifies the VLAN ID.

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
<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 case of MACs learnt on VXLAN tunnels or "port-access port-security" enabled ports, move scenario is handled by EVPN/port-access feature respectively and it performs the move by deleting the MAC from 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.

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.

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.

When used in mirror endpoint command context, specifies a comment for the mirror endpoint.

The **no** form of this command removes the comment.

Parameter	Description
<COMMENT>	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
```

Adding a comment to a mirror endpoint:

```
switch(config-mirror-endpoint-test)# comment Monitor endpoint traffic
```

Replacing the existing comment for mirror endpoint:

```
switch(config-mirror-endpoint-test)# comment Monitor statistics on each endpoint
interfaces
```

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-<SESSION-ID>` `config-mirror-endpoint`	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
<INTERFACE-ID>	Specifies a interface. Format: `member/slot/port`.
<LAG-NAME>	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.

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)
6000	1
6100	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

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
4100i 6000 6100	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.

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-<SESSION-ID>`	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-<SESSION-ID>`	Administrators or local user group members with execution rights for this command.

mirror endpoint

```
mirror endpoint <NAME>
no mirror endpoint <NAME>
```

Description

Creates the specified mirror endpoint or enters its context if it already exists. The specifics of a mirror endpoint are created or altered while in the mirror endpoint context and the mirror endpoint is enabled or disabled from this context. It may be possible to support different encapsulations by different ASICs. For example, UDP for PVOS compatibility. Termination of GRE encapsulation is also supported.

The **no** form of this command removes an existing mirror endpoint. An enabled mirror endpoint is automatically disabled first before removal.

Parameter	Description
<NAME>	Specifies mirror endpoint name.

Examples

Creating a mirror endpoint named test :

```
switch(config)# mirror endpoint test
```

Deleting mirror endpoint named test:

```
switch(config)# no mirror endpoint test
```

Configuring a mirror endpoint named test :

```
6100(config)# mirror endpoint test
6100(config-mirror-endpoint-test)#
6100(config-mirror-endpoint-test)# destination
```

```
  interface  Specify interfaces to send traffic
6100(config-mirror-endpoint-test)# destination interface
  IFNAMELIST  An interface, a range or a comma seperated list of interfaces
6100(config-mirror-endpoint-test)# destination interface 1/1/3
  <cr>
6100(config-mirror-endpoint-test)# destination interface 1/1/3
6100(config-mirror-endpoint-test)#
6100(config-mirror-endpoint-test)# source 1.1.1.1 destination 1.1.1.2 id 1 vrf
default
6100(config-mirror-endpoint-test)#
```

Only physical ports can be configured as interface for mirror-endpoint destination. LAG port is not supported as interface for mirror-endpoint destination.

The maximum allowed number of destination interfaces for both mirror-session and mirror-endpoint is 1.

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

Command History

Release	Modification
10.13.1000	Added support for 4100i, 6000, and 6100 switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	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
`<SESSION-ID>`	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)#
```

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>]`

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

Usage

Admin Status indicates the configured status. 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.

Operation Status 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
 Output Packets: 0
 Output Bytes: 0
switch#
```

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.

show mirror endpoint

```
show mirror endpoint [<NAME>]
```

Description

Shows a list of all configured mirror endpoints, their Admin Status and their Operation Status.

The optional parameter will display the details of the specified mirror endpoint if it exists.

Parameter	Description
<NAME>	Specifies name of the mirror endpoint instance to be displayed.

Examples

Showing a summary of all configured mirror endpoints on the switch:

```
switch# show mirror endpoint
Name    Admin Status   Operation Status
-----  -------------- ------------------------------------------------------
test    enable         enabled
monitor disable        disabled
```

Showing the details of enabled mirror endpoint test:

```
switch# show mirror endpoint test
Mirror Endpoint: audit
Admin Status: enable
Operation Status: enabled
Comment: Mirror Endpoint Audit
Type: gre
Tunnel: source 1.1.1.1 destination 1.1.1.2 id 1 vrf default
Interface: 1/1/3
Output Packets: 123456789
Output Bytes: 0
```

"Output Packets" in "show mirror endpoint [name]" is only supported for statistics.
"Output Bytes" in "show mirror endpoint [name]" is not supported due to ASIC limitation.

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

Command History

Release	Modification
10.13.1000	Added support for 4100i, 6000, and 6100 switches.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

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).
<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)
6000	52
6100	52

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.

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-*<SESSION-ID>*	Administrators or local user group members with execution rights for this command.

Chapter 52
MLD snooping global configuration commands

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

ipv6 mld snooping

```
ipv6 mld snooping {enable | disable}
no ipv6 mld snooping [enable | disable]
```

Description

This command enables or disables MLD snooping on the VLAN.

The **no** form of this command disables all MLD snooping configurations on the VLAN.

Parameter	Description
`enable`	Required: Enable MLD snooping on the VLAN.
`disable`	Required: Disable MLD snooping on the VLAN.

Example

Enable MLD snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping enable
switch(config-vlan)# ipv6 mld snooping disable
```

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
10.07 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.

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	`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
All platforms	`config-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping filter-unknown-mcast

```
ipv6 mld snooping filter-unknown-mcast
no ipv6 mld snooping filter-unknown-mcast
```

Description

Configures the unknown multicast to steal when the MLD snooping is enabled.

The **no** form of this command returns to the default behavior of initial flooding of unknown multicast traffic.

Usage

In the default behavior, the unknown multicast traffic is flooded until the IP Multicast Flow programming is done on the hardware. This is known as initial flooding of unknown multicast. Use this command to filter unknown multicast instead of flooding.

Initial flooding of multicast traffic is observed for a few seconds after the device comes up from a reboot. This issue is only seen when the multicast source connected device is rebooted. Once the device is up after a reboot, it takes a few seconds for the CPU Rx rule to be programmed during the timeframe that the initial flooding is observed. This is an expected behavior.

Example

Configure the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# ipv6 mld snooping filter-unknown-multicast
```

Removing the configuration of the unknown multicast to steal globally on IGMP snooping enabled VLANs.

```
switch# configure terminal
switch(config)# no ipv6 mld snooping filter-unknown-multicast
```

Command History

Release	Modification
10.14	Command introduced on the 4100i, 6000, and 6100 switch series.

Command Information

Platforms	Command context	Authority
6000 6100	config	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	`config-vlan`	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
`access-list`	Associates an ACL with the IGMP.
<ACL-NAME>	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	`config-vlan`	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
<VLAN-LIST>	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	`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	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	`config-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping preprogram-starg-flow

`ipv6 mld snooping preprogram-starg-flow {enable | disable}`

Description

This command configures the preprogramming of the starg flow feature on MLD snooping enabled VLANs.

Parameter	Description
`enable`	Enable preprogramming starg flows on the VLAN.
`disable`	Disable prprogramming starg flows on the VLAN.

Usage

When this feature is enabled, a summarized multicast bridge entry is programmed into the hardware table when a starg or sg MLD join is received on the MLD snooping enabled VLAN. This enables

multicast flow to be programmed in the hardware even before the data packet arrives for multicast flow. MLDv2 joins that are sent for a specific source are treated similar to starg joins and a summarized entry is programmed in the corresponding hardware.

Preprogramming of Starg Flows is supported only on the MLD snooping enabled VLANs. If MLD snooping is disabled on a VLAN, this feature is auto-disabled.

This feature is currently supported for MLDv1 and MLDv2 joins, which means a summarized multicast flow is programmed in advance when a MLDv1 or MLDv2 join for a specific group is received. For MLDv2 deployments, traffic from all of the sources for a specific multicast group are sent to all of the clients, regardless of whether they are sending MLDv1 or MLDv2 joins for this group. Keeping this feature disabled is recommended on VLANs where traffic from the specific source is only expected for the MLDv2 clients.

When an unknown multicast packet is received on a VLAN where the feature is enabled, it triggers programming of a starg entry in the hardware instead of SG.

On the 4100i, 6000, and 6100 switch series, a single starg entry is programmed in advance for each join received and data driven programming of SG entries occurs when the traffic is received from a specific source for this group. As a result, the starg entry is used to forward the initial traffic and the SG entries programmed in the multicast forwarding table are used to forward subsequent traffic to all of the clients (that have sent either MLDv2 joins or MLDv3 joins) for all of the active joins in the feature enabled VLANs.

It is highly recommended to not enable this feature on devices where PIM or L3 multicast routing is enabled as it can lead to issues like permanent traffic loss.

Configuring this feature on devices where there are multiple sources sending traffic for the same group address is recommended.

This feature is mutually exclusive with the MLD snooping static group feature.

Optimization may vary environment to environment, based on scale.

Example

Enable preprogramming of starg flow on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping preprogramming-starg-flow enable
```

Remove all preprogramming of starg flow on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping preprogramming-starg-flow disable
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config-vlan-<*VLAN-ID*>	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	config-vlan-<*VLAN-ID*>	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-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

show ipv6 mld snooping

```
show ipv6 mld snooping [vlan <vlan-id> [group <ip-addr>|{port <IF-NAME>}]
   counters
   detail
   groups vlan <vlan-id>
   no ...
   packet-exceptions
   static-groups
   statistics
```

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>`	Dispaly 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.
`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
`no ...`	Negates any configured parameter.
`packet-exceptions`	Troubleshoot issues in an L2 multicast bridge entries for data packets forwarded to the CPU.
`statistics`	Show MLD snooping statistics.

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

                                          V1        Sources   Sources
Port      Vers Mode Uptime    Expires     Timer     Forwarded 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	Manager (#)	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	`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
`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 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	`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 vlan 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	`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	`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	`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

```
6200-1(config-if-vlan)# ipv6 mld querier-wait-time
<1-300>  Querier Wait value (Default: 260)
6200-1(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 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	`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	`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. **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	`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	`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	`config-if-vlan`	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 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	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

Only the default VRF is supported on the Aruba 6000 and 6100 Switch Series.

show ipv6 mld

```
show ipv6 mld
   all-vrfs
   counters
   group <x:x::x:x> [source x:x::x:x]
   groups
   interface {<INTF-ID>}|{vlan <vlan-id}}
   static-groups
   statistics [all-vrfs|{vrf <vrf-name>}]
```

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 dislay 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
`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 for the selected VRF

Parameter	Description
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 forthe selcted VRF

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 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
```

```
                                V1          Sources   Sources
Vers Mode Uptime    Expires     Timer       Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    EXC  0m 14s    4m 6s
```

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
```

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
10.11	Sub-interface support extended to 8325 and 10000 Switch Series.
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.

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 vlan 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	`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 vlan 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	`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 vlan 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	`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 vlan 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	`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 `no ipv6 mld querier interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 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	`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 vlan 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	`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 vlan 1
switch(config-if)# ipv6 mld query-max-response-time 50
switch(config-if)# 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	`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 vlan 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	`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 vlan 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	`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 vlan 1
switch(config-if)# ipv6 mld version 2
```

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

Description

Shows priority, address, Hello-time, Max-age, and Forward-delay for bridge and root node.

Example

Showing spanning tree standard information:

```
switch# show spanning-tree
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    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 `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 detail

```
show spanning-tree detail
```

Description

Shows spanning tree detail including CIST and corresponding port information.

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 `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 [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: 0 to 64.

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
```

Description

Shows MSTP configuration and status information for each instance.

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     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

#### 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

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-config

```
show spanning-tree mst-config
```

Description

Shows MSTP instance and corresponding VLAN information.

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
```

Description

Shows detailed information for all MST instances.

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>`

Description

Displays MSTP configurations for the given instance ID.

Parameter	Description
<INSTANCE-ID>	Specifies the MSTP instance number. Range: 0 to 64.

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`

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 64.

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>`

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 64.
<IFNAME>	Specifies an interface.

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 `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 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

                                                    Root Hello Max Fwd
Instance ID     Priority Root ID                    cost  Time Age 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 bpdu-filter

```
spanning-tree bpdu-filter
no spanning-tree bpdu-filter
```

Description

Enables the bpdu 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 bpdu filter status to the default of disabled on the interface.

Examples

Enabling the bpdu filter on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree bpdu-filter
```

Disabling bpdu 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 on the interface. This is the default.

Parameter	Description
<INTERVAL>	Specifies the re-enable timeout in seconds. Range: 1 to 65535.

Example

Enabling the BPDU guard timeout on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree bpdu-guard timeout 10
```

Disabling BPDU guard timeout 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`	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: 1-64.
<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: 1-64.
<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 64.
<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 64.
<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
<AGE-IN-SECS>	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 priorites 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 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 64.
`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
  <0-64>  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
  <0-64>  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 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
<PORT-NUM>	Specifies a port number.
<PORT-LIST>	Specifies a list of ports.
LAG *<LAG-NUM>*	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
`join <TIME>`	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.
`leave <TIME>`	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.
`leaveall <TIME>`	Sets the leave all timer for the port, specifying the frequency with which the leave all state machine generates leave alll PDUs. Range: 500 to1000000 centiseconds. Default: 1000.
`periodic <TIME>`	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	`config-if`	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>]`

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.

Examples

```
switch# show mvrp config
Configuration and Status - MVRP
Global MVRP status : Disabled
Port    Status    Registration Join  Leave  LeaveAll Periodic
                  Type         Timer Timer  Timer    Timer
------- -------- --------      ----- -----  ------   --------
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>]
```

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>	
<PORT-NUM>	Specifies a physical port on the switch. Forrmat: **member/slot/port**.

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>]`

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.

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.

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}
    [{ <PLAINTXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
no ntp authentication-key <KEY-ID>  {md5 | sha1}
    [{ <PLAINTXT-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
<KEY-ID>	Specifies the authentication key ID. Range: 1 to 65534.
`md5`	Selects MD5 key encryption.
`sha1`	Specifies SHA1 key encryption.
<PLAINTXT-KEY>	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.
`trusted`	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.
`ciphertext` *<ENCRYPTED-KEY>*	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 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
`server <IP-ADDR>`	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** .
`key <KEY-NUM>`	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.
`minpoll <MIN-NUM>`	Specifies the minimum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 6 (64 seconds).
`maxpoll <MAX-NUM>`	Specifies the maximum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 10 (1024 seconds).
`burst`	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.
`iburst`	Send a burst of six packets when not connected to the server. Useful for reducing synchronization time at startup.
`prefer`	Make this the preferred server.
`version <VER-NUM>`	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.

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

6000 and 6100 only support default VRF.

Specifies the VRF on which the NTP client communicates with an NTP server.
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
```

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`

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).

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
```

Description

Shows the currently defined authentication keys.

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
```

Description

Shows all configured NTP servers, including any DHCP servers, default pool servers or any server with the status **auto prefer**.

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
```

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.

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`

Description

Shows the status of NTP on the switch.

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.

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}]
```

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.
`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.

Parameter	Description
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 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> |
   vrf <VRF-NAME> | source <IPv6-ADDR> | <IFNAME>]
```

Description

Pings the specified IPv6 address or hostname with or without optional parameters.

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.

Parameter	Description
`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
```

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

Platforms	Command context	Authority
	(#)	execution rights for this command. Operators can execute this command from the operator context (>) only.

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

crypto pki application

```
crypto pki application <APP-NAME> certificate <CERT-NAME>
no crypto pki application <APP-NAME> certificate <CERT-NAME>
```

Description

Associates a leaf certificate with a feature (application) on the switch. By default, all features are associated with the default, self-signed certificate **local-cert**. This certificate is created by the switch the first time it starts.

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: ▪ **dot1x-supplicant**: 802.1X supplicant ▪ **est-client**: EST client ▪ **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.
<CERT-NAME>	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-supplicant 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-<CERT-NAME>`	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.

Example

Enrolling the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# enroll terminal
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
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBozCCAQwCAQAwYzEVMBMGA1UEAxMMcG9kMDEtODQwMC0xMQ4wDAYDVQQLEwV
nViYTEMMAoGA1UEChMDSFBFMRIwEAYDVQQHEwlSb3NldmlsbGUxCzAJBgNVBAgT
NBMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtKcLS
...
GBAJ4L3lFFfWBEL+KAKpOGjZcVmwlBMqSKFtOFNF9nzmUmONmU3SKy6dzQ+6ynR
7Au22mf3lWDxzrtCC/dj5RtWJeJekxp2LCIK/3eRXUwbYveQDKcxH7j9ZB+BAp2
ace+2tA68F2vlgRCQ/hcQH0YmNuaq4Ne3w0dhm7HlUrx
-----END CERTIFICATE REQUEST-----
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-<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

Parameter	Description
	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)# HhcNMTkNDEwMjIwNT1WhcjIwMT0MjwNE1WjzQswQDVQQGEwJVUzEL
...
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/6rPspcjbx283iD1MWOpeoS2aEmOX
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-*<CERT-NAME>*	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.

Parameter	Description
	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)# tDCCA5ygAwIBAgICEAEwDQYJKoZIhvcNAQELBQAwgYgxCzABAYTAl
switch(config-cert-import)# VQQGEwJVUzELMAkGA1UECAwCQ0ExDTALBgNVBAcMBFJvc2UxDDAKB
...
switch(config-cert-import)# +fWQLxhp+jKJGZGOZz/FENt2uSfZHzlXiu8n3g+EgqExenY1pBRJr
switch(config-cert-import)# VuEEoNb/YfkPXHHva4Zfx223q+f694wlVsHkENSzqr2goHpa2fOzq
switch(config-cert-import)# alewwdmVqCES+x8bvhf3C/6IB6ePkEsnMlHNTeM=
switch(config-cert-import)# -----END CERTIFICATE-----
switch(config-cert-import)# -----BEGIN ENCRYPTED PRIVATE KEY-----
```

```
switch(config-cert-import)# MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIt8Ni3
switch(config-cert-import)# MBQGCCqGSIb3DQMHBAiBHrejkcdpdASCBMjVxrrYYPNt3V1abr9k8
switch(config-cert-import)# 5GE0U99awh9ys4360WR95xOFGThvjkTyRWG511nGwVeLZs/7TPXWI
...
switch(config-cert-import)# hzc5ZT/w2F08icRI5mFbGoTAAw9IIWMOXGweaWQJDyKGrhg89GrnV
switch(config-cert-import)# M2UuP/tYuuO328QcenKZEJmZKCbx78oFRR+pgma4oeMaFTIyXE6Pr
switch(config-cert-import)# GAdCK8tkDiJ9DKbqdM5W0/nTJfqwUQlfl27dNrBAodsHdrw3UR99H
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	`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 OCSP requests. A nonce is a unique identifier that an OCSP client inserts in an OCSP request and expects the OCSP responder to include it in the corresponding OCSP response. The nonce mechanism helps prevent replay attacks in which a malicious player attempts to masquerade as the OCSP 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)# ocsp enforcement-level optional
```

Setting strict OCSP checking of certificates:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# ocsp 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-<TA-NAME>`	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 OCSP responders. Default: **mgmt**.

Examples

Reverting the OCSP responder VRF to its default:

```
switch(config)# crypto pki ta-profile root-cert
switch(config-ta-root-cert)# no ocsp 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 ocsp

```
revocation-check ocsp
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 ocsp
```

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                      xhsccert               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.

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-test-1         installed      n/a               dot1x-supplicant
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-----

    MIICtTCCAZ0CAQAwcDEWMBQGA1UEAxMNc3lzbG9nLTg0MBYGA1UECxMPQ
    XJ1YmEtUm9zZXZpbGxlMQ4wDAYDVQQKEYTESMBAGA1EBxMJUm9zZXZpbG
    xlMQswCQYDVQQIEwJDQTELMAGA1UEBhMCVVMwggEiMSIb3DQEBAQUAA4I
    ...
    cw2ytN6Idgh81k59x6DH7V/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
  OCSP Secondary URL     : Not Configured
  OCSP Disable-nonce     : false
  OCSP Enforcement Level: strict
  OCSP 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.

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
`[import [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.

`import <REMOTE-URL>`	Import the certificate from a file on a remote TFTP or SFTP server. The URL syntax is:
	`{tftp:// | sftp://<USER>@} {<IP>|<HOST>}`
	`[:<PORT>] [;blocksize=<SIZE>]/<FILE>`

`import <STORAGE-URL>`	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)# VVMxEzARBgNVBAgMCkNhbGlmb3JuaWExEDAOBgNVBAcMB1JvY2tsDAKBg
switch(config-ta-cert)# BAoMA0hQTjEVMBMGA1UECwwMSFBOUm9zZXZpbGxlMSowKAYDVQocG5zdz
...
switch(config-ta-cert)# x3WFf3dFZ8o9sd5LVAHneH/ztb9MP34z+le1V346r12L2kpxmTOVJVyTO
switch(config-ta-cert)# BIzD/ST/HaWI+0S+S80rm93PSscEbb9GWk7vshh5EnW/moehBKcE4O1zy
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 (0xaea51217d5945772)

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 (0xaea51217d5945772)

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	config-ta-*<TA-NAME>*	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
`common-name <COMMON-NAME>`	Specifies the common name.
`country <COUNTRY>`	Specifies the country or region.
`locality <LOCALITY>`	Specifies the locality such as city.
`org <ORG-NAME>`	Specifies the organization.
`org-unit <ORG-UNIT>`	Specifies the organizational unit.
`state <STATE>`	Specifies the state.

Examples

Setting subject fields for the leaf certificate **leaf-cert**:

```
switch(config-cert-leaf-cert)# subject common-name Leaf01 country US
locality CA org Company org-unit Site 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 : Site
Enter Org Name : Company
Enter Locality : Rocklin
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	`config-cert-<CERT-NAME>`	Administrators or local user group members with execution rights for this command.

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

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	config-est-*<EST-NAME>*	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
<LABEL>	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
<EST-NAME>	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	`config`	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 be 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."

Parameter	Description
<EST-NAME>	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	`config-cert-<CERT-NAME>`	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 retires 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
<RETRIES>	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	config-est-*<EST-NAME>*	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
<INTERVAL>	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-<EST-NAME>`	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
<EST-NAME>	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
                                 Downloaded  Enrolled
Profile Name                     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
<USERNAME>	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.
ciphertext *<CIPHERTEXT-PASSWORD>*	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.
plaintext *<PLAINTEXT-PASSWORD>*	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
1DdyxAAQi4rmKr8LITMTTMd7qr
```

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.

All PoE configuration commands except **threshold configuration** and **always-on poe configuration** are entered at the **config-if** context. The PoE threshold command is used at the system level whereas the **always-on poe**and **power-over-ethernet quick-poe** commands are set at the slot level. These commands can only be configured in the global configuration context.

lldp dot3 poe

```
lldp dot3 poe
no lldp dot3 poe
```

Description

Enables 802.3 TLV list in LLDP to advertise for Power over Ethernet Data Link Layer Classification. LLDP dot3 TLV is by default enabled for PoE.

The **no** form of this command disables 802.3 TLV list in LLDP.

Examples

Enabling 802.3 TLV list in LLDP:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp dot3 poe
```

Disabling 802.3 TLV list in LLDP:

```
switch(config-if)# no lldp dot3 poe
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

lldp med poe

```
lldp med poe [priority-override]
no lldp med poe [priority-override]
```

Description

Enables MED TLV list in LLDP to advertise for Power over Ethernet Data Link Layer Classification. Also enables the lldp-MED TLV priority to override user configured port priority for Power over Ethernet. When both dot3 and MED are enabled, dot 3 will take precedence. MED TLV is by default enabled for PoE. Priority over-ride is by default disabled.

The **no** form of this command disables MED TLV list in LLDP.

Parameter	Description
`[priority-override]`	System defined name of the interface.

Examples

Enabling and disabling LLDP MED PoE:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp med poe
switch(config-if)# no lldp med poe
```

Enabling and disabling LLDP MED PoE priority override:

```
switch(config-if)# lldp med poe priority-override
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

power-over-ethernet

```
power-over-ethernet
no power-over-ethernet
```

Description

Enables per-interface power distribution. Per-port power is enabled by default with priority low. PoE cannot be disabled for individual ports when Quick PoE is enabled for the entire switch or line module.

The **no** form of this command disables per-interface power distribution.

Examples

Enabling per-interface power distribution:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet
```

Disabling per-interface power distribution:

```
switch(config-if)# no power-over-ethernet
```

Showing Quick PoE enabled:

```
switch(config-if)# power-over-ethernet quick-poe 1/1
switch(config-if)# interface 1/1/1
switch(config-if)# no power-over-ethernet
Interface PoE cannot be disabled when Quick PoE is enabled.
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet allocate-by

```
power-over-ethernet allocate-by {usage | class}
no power-over-ethernet allocate-by {usage | class}
```

Description

Configures the power allocation method. Power allocation method is initially based on usage. PSE Allocated power value will change to LLDP negotiated power if and when LLDP exchange takes place between PSE and PD. When there is no LLDP negotiation, PSE Allocated Power Value will be the actual instantaneous power draw and reserve power based on actual consumption. In allocate-by class, power allocation is based on PD requested class and PSE allocated power value will be the LLDP negotiated power when LLDP exchange takes place between PSE and PD. When there is no LLDP negotiation, PSE

Allocate Power will be based on PD class. Reserve power is based on PD Class. By default, power allocation is by usage.

The power allocation method can be changed on an interface through port-access (User roles or RADIUS). An allocation method when configured through port-access will replace the user configured method.

The **no** form of this command resets the action to default.

Parameter	Description
`usage`	Configures the usage-based allocation method.
`class`	Configures the class-based allocation method.

Usage

If you enable **pd-class-override** for an interface, the **allocate-by** configuration of that interface will be automatically changed to **class**. However, if you change the allocation method to **usage** when **pd-class-override** is still enabled, you will receive an error message stating that "The power allocation method cannot be changed when pd-class-override is enabled."

To remove **pd-class-override**, you can use the **no power-over-ethernet pd-class-override** command . It is important to note that **pd-class-override** requires the allocation method to be set to **class** and is enforced when configured through CLI. However, if you override the allocation method to **usage** via port-access, **pd-class-override** will not be in effect. Therefore, it is recommended that you do not override the allocation method to **usage** through port-access on interfaces configured with **pd-class-override**.

Examples

Configuring the power allocation method:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet allocate-by usage
switch(config-if)# power-over-ethernet allocate-by class
```

Resetting power allocation method:

```
switch(config-if)# no power-over-ethernet allocate-by class
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

power-over-ethernet assigned-class

```
power-over-ethernet assigned-class {3 | 4 | 6}
no power-over-ethernet assigned-class
```

Description

Limit PoE power based on the assigned class. When an user assigns a maximum class to an interface, the PSE will limit the maximum power delivered to the PD up to a total power draw not exceeding the PSE assigned-class power. Power demotion occurs when a PD requested class is higher than the PSE assigned class, permitting the PD to receive power and operate in a reduced power mode. PoE ports cannot set an assigned class when Quick PoE is enabled on the sybsystem. The default assigned class is 4 for 2-pair capable PSE and 6 for 4-pair capable PSE.

The **no** form of this command resets the action to default.

Examples

Setting PoE assigned class:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet assigned-class 4
```

Resetting PoE assigned class to default:

```
switch(config-if)# no power-over-ethernet assigned-class 4
```

Showing Quick PoE enabled:

```
switch(config)# power-over-ethernet quick-poe 1/1
switch(config)# interface 1/1/1
switch(config)# power-over-ethernet assigned-class 4
Interface assigned class cannot be configured when Quick PoE is enabled.
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet pre-std-detect

```
power-over-ethernet pre-std-detect
no power-over-ethernet pre-std-detect
```

Description

Before IEEE 802.3 released the first Power over Ethernet standard (802.3af), vendors had shipped PoE capable switches and PD's. As we are backward compatible Aruba will support both IEEE standard and pre-standard 802.3af Power over Ethernet PD's concurrently. This CLI allows the user to enable or disable pre-802.3af-standard device detection and powering on the specific port. When pre-std-detect is enabled, power will be delivered on PairA only. Default is disabled.

The **no** form of this command resets the action to default.

Examples

Enabling standard device detection:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet pre-std-detect
```

Disabling standard device detection:

```
switch(config-if)# no power-over-ethernet pre-std-detect
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet priority

```
power-over-ethernet priority {critical | high | low}
no power-over-ethernet priority {critical | high | low}
```

Description

Sets PoE priority for an interface Specifying critical, high, or low indicates the priority of the interface in the event of power over-subscription. Within the same priority level, higher power-priority line-module ports have higher precedence. With same PoE priority and same line-module priority, lower numbered line-module ports have higher precedence. Per-interface PoE priority is low by default.

The **no** form of this command resets the priority to default PoE priority "low".

Examples

Configuring PoE priority:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet priority critical
switch(config-if)# power-over-ethernet priority high
```

Resetting the PoE priority to default:

```
switch(config-if)# no power-over-ethernet priority high
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet threshold

```
power-over-ethernet threshold <PERCENTAGE>
no power-over-ethernet threshold <PERCENTAGE>
```

Description

Sets the threshold at which the system will send an excess power consumption notification trap. Default value is 80 percentage.

The **no** form of this command resets the action to default.

Parameter	Description
<PERCENTAGE>	Excess power consumption trap threshold. Range 1-99.

Examples

Setting the power-over-ethernet threshold:

```
switch(config)# power-over-ethernet threshold 75
```

Resetting the power-over-ethernet threshold to default:

```
switch(config-if)# no power-over-ethernet threshold 75
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

power-over-ethernet trap

```
power-over-ethernet trap
no power-over-ethernet trap
```

Description

This command enables/disables the SNMP trap generation for PoE related events at system level. PoE trap generation is enabled by default.

The **no** form of this command resets the priority to default PoE priority "low".

Examples

Enabling SNMP trap generation for PoE:

```
switch(config)# power-over-ethernet trap
```

Disabling SNMP trap generation for PoE:

```
switch(config-if)# no power-over-ethernet trap
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

show lldp local

`show lldp local-device [<INTERFACE-ID>]`

Description

Displays information advertised by the switch if the LLDP feature is enabled by user.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**

Examples

Showing LLDP local device:

```
switch# show lldp local-device 1/1/10
Local Port Data
===============

Port-ID           : 1/1/10
Port-Desc         : "1/1/10"
Port VLAN ID      : 0

PoE Plus Information

PoE Device Type    : Type 2 PSE
Power Source       : Primary
Power Priority     : low
PSE Allocated Power: 25.0 W
PD Requested Power : 25.0 W
```

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
6000 6100	Operator (>) or Manager (#)	Operators 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

```
show lldp neighbor [<INTERFACE-ID>]
```

Description

Displays detailed information about a particular neighbor connected to a particular interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**

Examples

Showing LLDP neighbor information when there is only one neighbor:

```
switch# show lldp neighbor-info 1/1/10

Port                           : 1/1/10
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 Aruba 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   :
Neighbor Port-ID               : 84:d4:7e:ce:5d:68
Neighbor Port-Desc             : eth0
TTL                            : 120
Neighbor Port VLAN ID          :
Neighbor PoEplus information   : DOT3
Neighbor Device Type           : TYPE2 PD
Neighbor Power Priority        : Unkown
Neighbor Power Source          : Primary
Neighbor Power Requested       : 25.0 W
Neighbor Power Allocated       : 0.0 W
Neighbor Power Supported       : No
Neighbor Power Enabled         : No
Neighbor Power Class           : 5
Neighbor Power Paircontrol     : No
Neighbor Power Pairs           : SIGNAL
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show power-over-ethernet

Description

Displays the status information of the full system.

Parameter	Description
`brief`	Display the brief status of all ports or the given port.

Examples

Showing sample output for show power-over-ethernet :

```
switch# show power-over-ethernet

System Power Status

  PoE  Power Status            : No redundancy
  Operational Power Status     : No redundancy
  Total Available Power        : 360 W
  Total Configured Power       :   0 W
  Total Failover Pwr Avl       :   0 W
  Total Redundancy Power       :   0 W
  Total Power Drawn            :   0 W
  Total Power Reserved         :   0 W
  Total Remaining Power        : 360 W
  Trap Threshold               : 80 %
  Trap Enabled                 : Yes
  Always-on PoE Enabled        : 1/1
  Quick PoE Enabled            : None


Internal Power
        Total Power
  PS    (Watts)        Status
  ----- -------------  ---------------------
  1/1   0              Ok
  1/2   0              Absent
```

Showing sample output for power-over-ethernet brief per-port:

```
switch# show power-over-ethernet 1/1/1 brief

Status and Configuration Information for port 1/1/1

  Member 1Power Status
    Available: 370 W  Reserved: 55.60 W  Remaining: 314.40 W
    Always-on PoE Enabled: 1/1
PoE      Pwr Power    Pre-std Alloc PSE Pwr PD Pwr PoE Port     PD     Cls Type
Port     En  Priority Detect  Act   Rsrvd   Draw   Status       Sign
-------  --- ------   ------- ----- ------  ------ ---------    -----  --- ----
1/1/1    Yes Low      Off     Class  0.0 W   0.0 W Denied       None   4   2
```

Showing sample output for power-over-ethernet brief for interface range:

```
switch# show power-over-ethernet 1/1/1-1/1/2 brief

Status and Configuration Information for port 1/1/1-1/1/2

    Power Status
    Available: 360 W  Reserved: 0.00 W  Remaining: 360.00 W
    Always-on PoE Enabled: 1/1
    Quick PoE Enabled: None
PoE      Pwr Power    Pre-std Alloc PSE Pwr PD Pwr PoE Port     PD     Cls Type
Port     En  Priority Detect  Act   Rsrvd   Draw   Status       Sign
-------  --- ------   ------- ----- ------  ------ ---------    -----  --- ----
1/1/1    Yes Low      Off     Usage  0.0 W   0.0 W Searching    N/A    N/A N/A
1/1/2    Yes Low      Off     Usage  0.6 W   0.0 W Searching    N/A    N/A N/A
```

Showing sample output for power-over-ethernet for a missing line card:

```
switch# show power-over-ethernet 1/3 brief

Module 1/3 is not physically present.
```

Showing sample output for power-over-ethernet port when physical interface is not present:

```
switch# show power-over-ethernet 2/1/1

Interface 2/1/1 is not present.
```

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
6000 6100	Operator (>) or Manager (#)	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 authentication port-access dot1x authenticator

```
aaa authentication port-access dot1x authenticator {enable | disable}
no aaa authentication port-access dot1x authenticator {enable | disable}
```

Description

Enables or disables 802.1X authentication globally or at the port-level.

The **no** form of the command deletes global 802.1X configuration details and disables 802.1X authentication.

Examples

Enabling 802.1X authentication globally:

```
switch(config)# aaa authentication port-access dot1x authenticator enable
```

Disabling 802.1X authentication globally:

```
switch(config)# aaa authentication port-access dot1x authenticator disable
```

Deleting and disabling global 802.1X authentication:

```
switch(config)# no aaa authentication port-access dot1x authenticator
```

Enabling 802.1X authentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator enable
```

Disabling 802.1X authentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator disable
```

Deleting and disabling 802.1X authentication configuration on a port:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator
```

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
6000 6100	`config` `config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator auth-method

```
aaa authentication port-access dot1x authenticator auth-method eap-radius
no aaa authentication port-access dot1x authenticator auth-method eap-radius
```

Description

Configures the authentication mechanism used to control access to the network. The configured authentication method will be used to authenticate 802.1X clients.

The **no** form of the command resets the authentication mechanism to the default, **eap-radius**.

Parameter	Description
`eap-radius`	Specifies the EAP RADIUS as the 802.1X authentication method.

Examples

Enabling the EAP RADIUS 802.1X authentication method on the switch:

```
switch(config)# aaa authentication port-access dot1x authenticator auth-method
eap-radius
```

Resetting the EAP RADIUS 802.1X authentication method on the switch:

```
switch(config)# no aaa authentication port-access dot1x authenticator auth-method
eap-radius
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator cached-reauth

```
aaa authentication port-access dot1x authenticator cached-reauth
no aaa authentication port-access dot1x authenticator cached-reauth
```

Description

Enables cached reauthentication on a port. Cached reauthentication allows 802.1X reauthentications to succeed when the RADIUS server is unavailable. Users already authenticated retain their currently assigned RADIUS attributes.

The **no** form of the command disables the cached reauthentication on a port.

Examples

Enabling cached reauthentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator cached-
reauth
```

Disabling cached reauthentication on a port:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator cached-
reauth
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator cached-reauth-period

```
aaa authentication port-access dot1x authenticator cached-reauth-period <PERIOD>
```

```
no aaa authentication port-access dot1x authenticator cached-reauth-period
```

Description

Configures the period during which an authenticated client, which has failed to reauthenticate because the RADIUS server is unreachable, remains authenticated.

The **no** form of the command resets the cached reauthentication period to the default, 30 seconds.

Parameter	Description
<PERIOD>	Specifies the cached reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring the cached reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator cached-reauth-period 300
```

Resetting the cached reauthentication period to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator cached-reauth-period
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator discovery-period

```
aaa authentication port-access dot1x authenticator discovery-period <PERIOD>
no aaa authentication port-access dot1x authenticator discovery-period
```

Description

Configures the period the port waits to retransmit the next EAPOL request identity frame on an 802.1X enabled port that has no authenticated clients.

The **no** form of the command resets the discovery period to the default, 30 seconds.

Parameter	Description
<PERIOD>	Specifies the discovery period (in seconds). Default: 30. Range: 1 to 65535.

Examples

Configuring the discovery period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator discovery-period 120
```

Resetting the discovery period to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator discovery-period
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator eap-tls-fragment

```
aaa authentication port-access dot1x authenticator eap-tls-fragment towards-server <max-fragment-size>
no aaa authentication port-access dot1x authenticator eap-tls-fragment towards-server
```

Description

Configure the maximum size in bytes of an EAP-TLS fragment encoded in a single RADIUS request packet. The **no** form of the command resets the size to the default value of 3072 bytes.

Examples

Setting the EAP-TLS fragment size for RADIUS request to 1024 bytes:

```
switch(config)# aaa authentication port-access dot1x authenticator eap-tls-
fragment towards-server 1024
```

Resetting EAP-TLS fragment size back to the default value of 3072 bytes

```
switch(config-if)# no aaa authentication port-access dot1x authenticator eap-tls-
fragment towards-server
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator eapol-timeout

```
aaa authentication port-access dot1x authenticator eapol-timeout <EAPOL-TIMEOUT>
no aaa authentication port-access dot1x authenticator eapol-timeout
```

Description

Configure the period the switch waits for a response from a client before retransmitting an EAPOL PDU. If the value is **0**, the time period is calculated as per RFC 2988.

As per RFC 2988 2.1: Before Round-Trip Time (RTT) measurement, set Retransmission Timeout (RTO) to 3 seconds for initial retransmission and then double the RTO to provide back off as per section 5.5. Limit the maximum RTO (RTOmax) to 20 seconds as per section 4.3 of RFC 3748.

The **no** form of the command resets the timeout period to the default.

Parameter	Description
<EAPOL-TIMEOUT>	Specifies the EAPOL timeout period (in seconds). Range: 1 to 65535.

Examples

Configuring EAPOL timeout on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator eapol-
timeout 120
```

Resetting the EAPOL timeout to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator eapol-
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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator initial-auth-response-timeout

```
aaa authentication port-access dot1x authenticator
    initial-auth-response-timeout <TIMEOUT>
no aaa authentication port-access dot1x authenticator
    initial-auth-response-timeout [<TIMEOUT>]
```

Description

Configures the period of time (in seconds) the switch waits for the first EAPOL frame from a client before deeming the client to be incapable of 802.1X and therefore attempting the next authentication method, if any. The default is for this timeout to be disabled.

The **no** form of this command disables the timeout.

Parameter	Description
<TIMEOUT>	Specifies the timeout period (in seconds). Range: 1 to 65535.

Examples

Setting a 30 second timeout:

```
switch(config-if)# aaa authentication port-access dot1x authenticator
   initial-auth-response-timeout 30
```

Disabling the timeout:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator
   initial-auth-response-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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator max-eapol-requests

```
aaa authentication port-access dot1x authenticator max-eapol-requests <MAX-EAPOL-REQUESTS>
no aaa authentication port-access dot1x authenticator max-eapol-requests
```

Description

Configures the number of EAPOL requests to send to a supplicant that must time out before authentication fails and the authentication session ends.

The **no** form of the command resets the maximum number of EAPOL requests to the default, 5.

Parameter	Description
<MAX-EAPOL-REQUESTS>	Specifies the maximum number of EAPOL requests. Default: 5. Range: 1 to 10.

Examples

Configuring maximum EAPOL requests on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator max-eapol-
requests 3
```

Resetting the maximum EAPOL requests on a port to default:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator max-
eapol-requests
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator max-retries

```
aaa authentication port-access dot1x authenticator max-retries <max-retries>
no aaa authentication port-access dot1x authenticator max-retries
```

Description

Configures the maximum number of retries that the switch attempts to authenticate a client on a port before marking the client as unauthenticated.

The **no** form of the command resets the maximum number of retries to the default, 2.

Parameter	Description
<max-retries>	Indicates the number of authentication attempts. Default: 2. Range: 1 to 10.

Examples

Configuring maximum authentication attempts on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator max-retries
5
```

Resetting the maximum authentication attempts on a port to default:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator max-
retries
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator quiet-period

```
aaa authentication port-access dot1x authenticator quiet-period <PERIOD>
no aaa authentication port-access dot1x authenticator quiet-period
```

Description

Configures the period during which the port does not try to acquire a supplicant. This period begins after the last authentication attempt, authorized by the maximum retries parameter, fails.

You can configure the number of maximum retries with the **aaa authentication port-access dot1x authenticator max-retries** command.

The **no** form of the command resets the quiet period to the default, 60 seconds.

Parameter	Description
<PERIOD>	Specifies the quiet period (in seconds). Default: 60. Range: 0 to 65535.

Examples

Configuring quiet period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator quiet-period
100
```

Resetting the quiet period on a port to default:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator quiet-
period
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator radius server-group

```
aaa authentication port-access dot1x authenticator radius server-group <GROUP-NAME>
no aaa authentication port-access dot1x authenticator radius server-group <GROUP_NAME>
```

Description

Configures the switch to use an existing RADIUS server group for 802.1X authentication globally or for a particular port.

The **no** form of the command resets the server group to the default, **radius**.

When configured on a port, the **no** form of the command resets the server group on that port to the globally configured group. If no global RADIUS server group is configured, the **no** form of the command resets the configuration to the default group, **radius**.

When the RADIUS server group for 802.1X authentication is updated on a port, any existing clients on the port that were authenticated using the previous globally configured group will associate with the new group for the port during the next re-authentication cycle. Any new client that is onboarding on the port after the server group update will associate with the new group immediately.

Parameter	Description
<GROUP-NAME>	Specifies the name of the RADIUS server group.

Examples

Configuring the switch to use RADIUS server group **employee**:

```
switch(config)# aaa authentication port-access dot1x authenticator radius server-
group employee
```

Resetting RADIUS server group configuration to default:

```
switch(config)# no aaa authentication port-access dot1x authenticator radius
server-group
```

Configuring the RADIUS authentication server group on **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# radius server-group group2
```

Resetting 802.1X RADIUS server group configuration on **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x authenticator
switch(config-if-dot1x-auth)# no radius server-group
```

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 is now configurable on a port
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-dot1x-auth`
	`config-if-dot1x-auth`
		Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator reauth

```
aaa authentication port-access dot1x authenticator reauth
no aaa authentication port-access dot1x authenticator reauth
```

Description

Enables periodic reauthentication of authenticated clients on the port.

The **no** form of the command disables periodic reauthentication.

Examples

Enabling periodic reauthentication on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator reauth
```

Disabling periodic reauthentication on a port:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator reauth
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x authenticator reauth-period

```
aaa authentication port-access dot1x authenticator reauth-period <PERIOD>
no aaa authentication port-access dot1x authenticator reauth-period
```

Description

Configures the period after which the authenticated clients are reauthenticated on the port. You must enable reauthentication on the port before configuring the reauthentication period.

The **no** form of the command resets the reauthentication period to the default, 3600 seconds.

Parameter	Description
<PERIOD>	Specifies the reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access dot1x authenticator reauth-
period 100
```

Resetting the reauthentication period to the default value:

```
switch(config-if)# no aaa authentication port-access dot1x authenticator reauth-
period
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

clear dot1x authenticator statistics interface

`clear dot1x authenticator statistics [interface <IF-NAME>]`

Description

Clears the 802.1X authentication statistics associated with the port and all the authenticator clients attached to this port.

If no interface is specified, the statistics is cleared for all 802.1X enabled ports.

Parameter	Description
<IF-NAME>	Specifies the interface name.

Examples

Clearing authentication statistics on a port:

```
switch# clear dot1x authenticator statistics interface 1/1/1
```

Clearing authentication statistics on a port:

Clearing authentication statistics on all ports:

```
switch# clear dot1x authenticator statistics
```

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
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show aaa authentication port-access dot1x authenticator interface client-status

```
show aaa authentication port-access dot1x authenticator interface {all|<IF-NAME>}
     client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about active 802.1X authentication sessions. The output can be filtered by interface or MAC address.

Parameter	Description
`all`	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing client status information for all ports.

```
switch# show aaa authentication port-access dot1x authenticator interface all
client-status

Client  FE:04:D7:50:89:37, johndoe, 1/1/1
==========================================

  Authentication Details
  ----------------------
    Status                        : Authenticated
    Type                          : Pass-Through
    EAP-Method                    : MD5
    Time Since Last State Change  : 10s

  Authentication Statistics
  -------------------------
    Authentication                          : 0
    Authentication Timeout                  : 0
    EAP-Start While Authenticating          : 0
    EAP-Logoff While Authenticating         : 0
    Successful Authentication               : 0
    Failed Authentication                   : 0
    Re-Authentication                       : 0
    Successful Re-Authentication            : 0
    Failed Re-Authentication                : 0
    EAP-Start When Authenticated            : 0
    EAP-Logoff When Authenticated           : 0
    Re-Auths When Authenticated             : 0
    Cached Re-Authentication                : 0
```

```
Client  9A:B4:59:97:D0:7E, janedoe, 1/1/1
========================================

  Authentication Details
  ----------------------
    Status                        : Authenticated
    Type                          : Pass-Through
    EAP-Method                    : TLS
    Time Since Last State Change  : 5s

  Authentication Statistics
  -------------------------
    Authentication                          : 0
    Authentication Timeout                  : 0
    EAP-Start While Authenticating          : 0
    EAP-Logoff While Authenticating         : 0
    Successful Authentication               : 0
    Failed Authentication                   : 0
    Re-Authentication                       : 0
    Successful Re-Authentication            : 0
    Failed Re-Authentication                : 0
    EAP-Start When Authenticated            : 0
    EAP-Logoff When Authenticated           : 0
    Re-Auths When Authenticated             : 0
    Cached Re-Authentication                : 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
6000 6100	Operator (>) or Manager (#)	Operators 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 port-access dot1x authenticator interface port-statistics

`show aaa authentication port-access dot1x authenticator interface {all|<IF-NAME>} port-statistics`

Description

Shows information about 802.1X ports. The output can be filtered by interface.

Parameter	Description
`all`	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show aaa authentication port-access dot1x authenticator interface all
port-statistics

Port 1/1/1
==========

  Client Details
  --------------
    Number of Clients                 : 1
    Number of Authenticated Clients   : 1
    Number of Unauthenticated Clients : 0
    Number of authenticating clients  : 0


  Statistics
  ----------
    EAPOL Frames Received                  : 4
    EAPOL Frames Transmitted               : 3
    EAPOL Start Frames Received            : 1
    EAPOL Logoff Frames Received           : 0
    EAPOL Response ID Frames Received      : 2
    EAPOL Response Frames Received         : 1
    EAPOL Request ID Frames Transmitted    : 2
    EAPOL Request Frames Transmitted       : 1
    EAPOL Invalid Frames Received          : 0
    EAPOL EAP Length Error Frames Received : 0
    EAPOL Last Received Frame Version      : 0
    EAPOL Last Received Frame Client MAC   : 0

Port 1/1/2
==========

  Client Details
  --------------
    Number of Clients                 : 1
    Number of Authenticated Clients   : 1
    Number of Unauthenticated Clients : 0

  Statistics
  ----------
    EAPOL Frames Received                  : 4
    EAPOL Frames Transmitted               : 3
    EAPOL Start Frames Received            : 1
    EAPOL Logoff Frames Received           : 0
    EAPOL Response ID Frames Received      : 2
    EAPOL Response Frames Received         : 1
    EAPOL Request ID Frames Transmitted    : 2
    EAPOL Request Frames Transmitted       : 1
    EAPOL Invalid Frames Received          : 0
    EAPOL EAP Length Error Frames Received : 0
```

```
   EAPOL Last Received Frame Version      : 0
   EAPOL Last Received Frame Client MAC   : 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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 66
Port access 802.1X supplicant commands

aaa authentication port-access dot1x supplicant (global)

```
aaa authentication port-access dot1x supplicant
```

Description

Enters the 802.1X supplicant global configuration context.

Example

Enter the 802.1X supplicant configuration context:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	`config` `config-dot1x-supp`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access dot1x supplicant (port)

```
aaa authentication port-access dot1x supplicant
```

Description

Enters the 802.1X supplicant port context.

The 802.1X supplicant is only supported on L2 physical interfaces that are not members of a LAG.

Example

Enter the 802.1X supplicant port context:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)#
```

When entering the context on a L3 port, an error message displays:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
The operation is allowed only on a L2 physical interface.
```

When entering the context on a LAG, an error message displays:

```
switch(config)# interface lag 1
switch(config-if)# aaa authentication port-access dot1x supplicant
The operation is allowed only on a L2 physical interface.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-if config-dot1x-supp	Administrators or local user group members with execution rights for this command.

associate policy

```
associate policy <POLICY-NAME>
no associate policy <POLICY-NAME>
```

Description

Associates a supplicant policy with the port.

The **no** form of the command dissociates the policy from the port and reverts to the default policy.

If an 802.1X supplicant is enabled on the port without associating a policy or dissociating a policy from the port, it results in the port using the default policy.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy. (Maximum 32 characters).

Examples

Associating a supplicant policy with the port:

```
switch(config)# interface 1/1/1
switch(config)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# associate policy CX_Policy
```

Removing the supplicant policy on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no associate policy
OR

switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no associate policy CX_Policy
```

When the policy being associated does not exist:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# associate policy New_Supp_Policy
The policy does not exist.
```

When the policy being dissociated is not the one configured on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# associate policy New_Supp_Policy
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

canned-eap-success

```
canned-eap-success
no canned-eap-success
```

Description

Configures the switch to accept an EAP success from the authenticator without going through the complete authentication cycle. Default: disabled.

The **no** form of the command resets it to the default.

Examples

Configuring the switch to accept a canned EAP success:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# canned-eap-success
```

Resetting the allow canned EAP success configuration to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no canned-eap-success
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

clear dot1x supplicant statistics

```
clear dot1x supplicant statistics [interface <IFRANGE>]
```

Description

Clears the 802.1X supplicant statistics associated with the interface. If no interface is specified, the statistics are cleared for all 802.1X supplicant-enabled interfaces.

Parameter	Description
<IFRANGE>	Specifies the range of VLAN interfaces for which the supplicant statistics are cleared.

Examples

Clearing authenticator statistics on a specific interface:

```
switch# clear dot1x supplicant statistics 1/1/1
```

Clearing authenticator statistics on all interfaces:

```
switch# clear dot1x supplicant statistics
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# clear dot1x supplicant statistics
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the interface:

```
switch# clear dot1x supplicant statistics 1/1/1
802.1X supplicant is not configured.
```

Showing the message when there are no 802.1X supplicants on the system:

```
switch# clear dot1x supplicant statistics
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# clear dot1x supplicant statistics 1/1/1
No 802.1X supplicants found.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

discovery-timeout

```
discovery-timeout <DISCOVERY-TIMEOUT>
no discovery-timeout <DISCOVERY-TIMEOUT>
```

Description

Configures the time period (in seconds) to wait for a potential 802.1X authenticator on the other end before considering the link to be non-802.1X-capable and opening the interface on the data-plane. On a timeout, the switch will not use the authentication result to determine the forwarding behavior of the interface until a link flap. If not set, the switch will wait for the 802.1X authentication cycle to complete before determining the forwarding state of the interface.

The **no** form of the command removes the configuration.

Parameter	Description
<DISCOVERY-TIMEOUT>	Specifies discovery timeout in seconds. Range: 0-300 seconds.

Examples

Configuring a discovery timeout of 15 seconds in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# discovery-timeout 15
```

Removing the discovery timeout from the policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no discovery-timeout

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no discovery-timeout 15
```

When the value entered does not match the currently configured non-default value for EAPoL timeout, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
```

```
switch(config-dot1x-supp-policy)# discovery-timeout 15
switch(config-dot1x-supp-policy)# no discovery-timeout 5
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eap-identity

```
eap-identity identity <IDENTITY>
no eap-identity identity <IDENTITY>
eap-identity password {plaintext [<PLAINTEXT-PASSWORD>] | ciphertext <CIPHERTEXT-PASSWORD>}
no eap-identity password {plaintext [<PLAINTEXT-PASSWORD>] | ciphertext <CIPHERTEXT-PASSWORD>}
```

Description

Configures the EAP identity to use for authentication including an identity name and an optional password.

The **no** form of the command removes the configuration.

Parameter	Description
<IDENTITY>	Specifies the EAP identity name. Maximum: 64 characters.
<PLAINTEXT-PASSWORD>	Specifies the password associated with the EAP identity in plaintext. Maximum: 32 characters. 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.
<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 *<CIPHERTEXT-PASSWORD>* is Base64 and is typically copied from another switch using the `show running-config` command output and then pasted into this command.

Parameter	Description
	NOTE: 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 `user` command. The ciphertext is available for copying from the `show running-config` 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.

Examples

Configuring the EAP identity and password:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity John Doe
switch(config-dot1x-supp-policy)# eap-identity password plaintext johndoe

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity John Doe
switch(config-dot1x-supp-policy)# eap-identity password plaintext
Enter password: ******
Confirm password: ******

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity John Doe
switch(config-dot1x-supp-policy)# eap-identity password ciphertext
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
```

Removing the EAP identity configuration:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eap-identity identity

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-identity identity John Doe
```

Removing the EAP identity password configuration:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-identity password

OR

switch(config)# aaa authentication port-access dot1x supplicant
```

```
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-identity ciphertext
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
```

When the EAP identity string is longer than 64 characters, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity identity This is a really long
string with more than sixty four characters in it
The EAP identity string is more than 64 characters long.
```

When the EAP identity password string is longer than 32 characters, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-identity password plaintext This is a
password with more than 32 characters
The password is more than 32 characters long.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-force-multicast

```
eapol-force-multicast
no eapol-force-multicast
```

Description

Configures the switch to send only multicast EAPoL packets irrespective of receiving unicast EAPoL packets from the authenticator. Default: disabled.

The **no** form of the command resets it to the default.

Examples

Configuring the switch to always send EAPoL multicast packets:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-force-multicast
```

Resetting the EAPoL force multicast setting to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-force-multicast
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-dot1x-supp`
	`config-dot1x-supp-policy`
		Administrators or local user group members with execution rights for this command.

eapol-method

```
eapol-method {eap-tls | eap-md5}
no eapol-method {eap-tls | eap-md5}
```

Description

Configures the Extensible Authentication Protocol (EAP) method to use for authentication.

The **no** form of the command resets it to the default. The default is EAP-TLS.

Parameter	Description
`eapol-method`	Specifies the EAPoL method to use for authentication. Default: eap-tls.
`eap-tls`	Specifies the EAP method as EAP with TLS (EAP with transport layer security)
`eap-md5`	Specifies the EAP method as EAP with MD5 digest.

Examples

Configuring the EAP method as EAP-MD5:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-method eap-md5
```

Resetting the EAP method to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eap-method

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eap-method eap-md5
```

When the value entered does not match the currently configured non-default value for EAP method, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eap-method eap-md5
switch(config-dot1x-supp-policy)# no eap-method eap-tls
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

eapol-protocol-version

```
eapol-protocol-version
no eapol-protocol-version
```

Description

Configures the EAPoL protocol version to use in EAPoL frames transmitted by the supplicant.

The **no** form of the command resets it to the default.

When the EAPoL protocol version is modified while the policy is in use on one or more ports, all the supplicant sessions on such ports are restarted.

Parameter	Description
protocol-version	Required. Specifies the protocol-version. Options: 2 or 3. Default: 3.

Examples

Configuring the EAPoL protocol version as 2 in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-protocol-version 2
```

Reset the EAPoL protocol version to the default value:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eapol-protocol-version

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-protocol-version 2
```

When the value entered does not match the currently configured non-default value for EAPoL protocol version, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-protocol-version 2
switch(config-dot1x-supp-policy)# no eapol-protocol-version 3
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-dot1x-supp`
	`config-dot1x-supp-policy`
		Administrators or local user group members with execution rights for this command.

eapol-timeout

```
eapol-timeout <EAPOL-TIMEOUT>
no eapol-timeout <EAPOL-TIMEOUT>
```

Description

Configures the time period (in seconds) to wait for a response from an authenticator before reattempting authentication.

The **no** form of the command resets it to the default.

Parameter	Description
<EAPOL-TIMEOUT>	Specifies EAPoL timeout in seconds. Default: 30 seconds.

Examples

Configuring an EAPoL timeout of 10 seconds in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-timeout 10
```

Resetting the EAPoL timeout to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no eapol-timeout

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no eapol-timeout 10
```

When the value entered does not match the currently configured non-default value for EAPoL timeout, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# eapol-timeout 10
switch(config-dot1x-supp-policy)# no eapol-timeout 5
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-dot1x-supp`
	`config-dot1x-supp-policy`
		Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables the 802.1X supplicant on the port. By default, the 802.1X supplicant is disabled on the port.

The **no** form of the command disables the 802.1X supplicant on the port.

Example

Enable the 802.1X supplicant on the port:

```
switch(config)# interface 1/1/1
switch(config)# no routing
switch(config-if)# aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# enable
```

Disable the 802.1X supplicant on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access dot1x supplicant
switch(config-if-dot1x-supp)# no enable
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables the 802.1X supplicant on the system. By default, 802.1X supplicant is disabled on the system.

The **no** form of the command disables the 802.1X supplicant on the system.

Example

Enable the 802.1X supplicant on the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# enable
```

Disable the 802.1X supplicant on the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# no enable
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp	Administrators or local user group members with execution rights for this command.

fail-mode

```
fail-mode [fail-closed | fail-open]
no fail-mode [fail-closed | fail-open]
```

Description

Configures the forwarding behavior of the when the 802.1X authentication fails. Default: fail-open.

The **no** form of the command resets it to the default.

Examples

Configuring the fail mode as fail-closed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# fail-mode fail-closed
```

Resetting the fail mode to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no fail-mode

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no fail-mode fail-closed
```

When the fail-mode value entered does not match the currently configured non-default value:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# fail-mode fail-closed
switch(config-dot1x-supp-policy)# no fail-mode fail-open
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

held-period

```
held-period <HELD-PERIOD>
no held-period <HELD-PERIOD>
```

Description

Configure the time period (in seconds) to wait after a failed authentication attempt before another attempt is permitted.

The **no** form of the command resets it to default.

Parameter	Description
<HELD-PERIOD>	Specifies the held period in seconds. Default: 60 seconds.

Usage

When the value entered does not match the currently configured non-default value for held-period, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# held-period 30
switch(config-dot1x-supp-policy)# held-period 50
The input value does not match the currently configured value.
```

Examples

Configuring a held period of 30 seconds in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# held-period 30
```

Resetting the held period to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no held-period

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no held-period 30
```

When the value entered does not match the currently configured non-default value for held-period, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# held-period 30
switch(config-dot1x-supp-policy)# held-period 50
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-dot1x-supp`
	`config-dot1x-supp-policy`
		Administrators or local user group members with execution rights for this command.

max-retries

```
max-retries <MAX-RETRIES>
no max-retries <MAX-RETRIES>
```

Description

Configures the maximum number of authentication attempts before authentication fails.

The **no** form of the command resets it to the default.

Parameter	Description
<MAX-RETRIES>	Specifies the maximum retry attempts allowed. Range: 1-5. Default: 2.

Examples

Configuring the maximum retries to 5 in the supplicant policy:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# max-retries 5
```

Resetting the max retries to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp)# no max-retries

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no max-retries 5
```

When the value entered does not match the currently configured non-default value for max-retries, the following message is displayed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
```

```
switch(config-dot1x-supp-policy)# max-retries 5
switch(config-dot1x-supp-policy)# max-retries 3
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

policy (supplicant)

```
policy <POLICY-NAME>
no policy <POLICY-NAME>
```

Description

Creates an 802.1X supplicant policy on the system.

The **no** form of the command deletes the 802.1X supplicant policy on the system.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy. (Maximum 32 characters).

Usage

Configure an 802.1X supplicant policy on the system:

Examples

Configure an 802.1X supplicant policy on the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)#
```

Delete the 802.1X supplicant policy from the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# no policy CX_Policy
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	config config-dot1x-supp config-dot1x-supp-policy	Administrators or local user group members with execution rights for this command.

port-access dot1x supplicant restart

```
port-access dot1x supplicant restart [interface <IFRANGE>]
```

Description

Restarts the 802.1X supplicant on the specified interface. The current authentication state is discarded and the supplicant restarts the authentication process.

Parameter	Description
<IFRANGE>	Optional. Specifies the range of physical interfaces for which the supplicant is restarted.

Examples

Restarting the 802.1X supplicant on a specific interface:

```
switch# port-access dot1x supplicant restart interface 1/1/1
switch#
```

Restarting the 802.1X supplicant on all interfaces:

```
switch# port-access dot1x supplicant restart
switch#
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# port-access dot1x supplicant restart
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the given interface:

```
switch# port-access dot1x supplicant restart 1/1/1
802.1X supplicant is not configured.
```

Showing the message when there are no 802.1X supplicants on the system:

```
switch# port-access dot1x supplicant restart
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# port-access dot1x supplicant restart 1/1/1
No 802.1X supplicants found.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 port-access dot1x supplicant policy

`show aaa authentication port-access dot1x supplicant policy <POLICY-NAME>`

Description

Shows information about the 802.1X supplicant policies on the system.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy. (Maximum 32 characters).

Examples

Showing all 802.1X supplicant policies on the system:

```
switch# show aaa authentication port-access dot1x supplicant policy

802.1X Supplicant Policy Details

  Policy Name: default
  ------------------------------------------------------------------------------
  Type                      : Default
  EAP Method                : EAP-TLS
  Held Period               : 60 seconds
  Maximum Retries           : 2
  EAPoL Timeout             : 30 seconds
  EAP Identity              : --
  EAP Identity Password     : --
  EAPoL Force Multicast     : False
  EAPoL Protocol Version    : 3
  Canned EAP Success        : False
  Discovery Timeout         : --
  Start Mode                : Start-Open
  Fail Mode                 : Fail-Open
  MACsec Policy             : --

  Policy Name: CX_Policy
  ------------------------------------------------------------------------------
  Type                      : Static
  EAP Method                : EAP-MD5
  Held Period               : 30 seconds
  Maximum Retries           : 5
  EAPoL Timeout             : 10 seconds
  EAP Identity              : John Doe
  EAP Identity Password     :
QBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
  EAPoL Force Multicast     : True
  EAPoL Protocol Version    : 2
  Canned EAP Success        : True
  Discovery Timeout         : 15 seconds
  Start Mode                : Start-Closed
  Fail Mode                 : Fail-Closed
  MACsec Policy             : Aggregator-Connect
```

Showing a specific 802.1X supplicant policy:

```
switch# show aaa authentication port-access dot1x supplicant policy CX_Policy

802.1X Supplicant Policy Details

  Policy Name: CX_Policy
  ------------------------------------------------------------------------------
  Type                      : Static
  EAP Method                : EAP-MD5
  Held Period               : 30 seconds
  Maximum Retries           : 5
  EAPoL Timeout             : 10 seconds
  EAP Identity              : John Doe
  EAP Identity Password     :
AQBapUwNK5Uf+r1vmhBIncQPw1YPVH0V1nYr7Yjm/bPn3bBVCgAAAHFKt8mcSv/A/g8=
  EAPoL Force Multicast     : True
  EAPoL Protocol Version    : 2
```

```
  Canned EAP Success       : True
  Discovery Timeout        : 15 seconds
  Start Mode               : Start-Closed
  Fail Mode                : Fail-Closed
  MACsec Policy            : Aggregator-Connect
```

If the policy with given name does not exist:

```
switch# show aaa authentication port-access dot1x supplicant policy New_CX_Policy
The policy does not exist.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 port-access dot1x supplicant statistics

```
show aaa authentication port-access dot1x supplicant statistics
[interface {<IFRANGE> | vlan <VLAN-ID>}]
```

Description

Shows the 802.1X supplicant statistics on each 802.1X supplicant-enabled interface.

Parameter	Description
<IFRANGE>	Specifies the range of VLAN interfaces for which the supplicant status is shown.
`vlan` *<VLAN-ID>*	Specifies a VLAN interface for which the supplicant status is shown.

Examples

Showing the 802.1X supplicant statistics on all enabled interfaces:

```
switch# show aaa authentication port-access dot1x supplicant statistics

802.1X Supplicant Statistics

Interface 1/1/1
===================

  EAPOL Frames Received                  : 4
  EAPOL Frames Transmitted               : 3
  EAPOL Start Frames Transmitted         : 1
  EAPOL Logoff Frames Transmitted        : 0
  EAPOL Invalid Frames Received          : 0
  EAPOL EAP Length Error Frames Received : 0
  Authentication                         : 0
  Authentication Timeout                 : 0
  EAP-Logoff While Authenticating        : 0
  Successful Authentication              : 0
  Failed Authentication                  : 0
  Re-Authentication                      : 0
  EAP-Logoff When Authenticated          : 0

Interface 1/1/2
===================

  EAPOL Frames Received                  : 0
  EAPOL Frames Transmitted               : 1
  EAPOL Start Frames Transmitted         : 1
  EAPOL Logoff Frames Transmitted        : 0
  EAPOL Invalid Frames Received          : 0
  EAPOL EAP Length Error Frames Received : 0
  Authentication                         : 0
  Authentication Timeout                 : 0
  EAP-Logoff While Authenticating        : 0
  Successful Authentication              : 0
  Failed Authentication                  : 0
  Re-Authentication                      : 0
  EAP-Logoff When Authenticated          : 0
```

Showing the 802.1X supplicant status on a specific interface:

```
switch# show aaa authentication port-access dot1x supplicant statistics interface
1/1/1

802.1X Supplicant Statistics

Interface 1/1/1
===================

  EAPOL Frames Received                  : 4
  EAPOL Frames Transmitted               : 3
  EAPO Start Frames Transmitted          : 1
  EAPOL Logoff Frames Transmitted        : 0
  EAPOL Invalid Frames Received          : 0
  EAPOL EAP Length Error Frames Received : 0
  Authentication                         : 0
  Authentication Timeout                 : 0
  EAP-Logoff While Authenticating        : 0
  Successful Authentication              : 0
  Failed Authentication                  : 0
  Re-Authentication                      : 0
  EAP-Logoff When Authenticated          : 0
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# show aaa authentication port-access dot1x supplicant statistics
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the interface:

```
switch# show aaa authentication port-access dot1x supplicant statistics interface
1/1/1
802.1X supplicant is not configured.
```

Showing the message when there are no 802.1X supplicants on the system:

```
switch# show aaa authentication port-access dot1x supplicant status
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface
1/1/1
No 802.1X supplicants found.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 port-access dot1x supplicant status

```
show aaa authentication port-access dot1x supplicant status
[interface {<IFRANGE> | vlan <VLAN-ID>}]
```

Description

Shows the 802.1X supplicant status on each 802.1X supplicant-enabled interface.

Parameter	Description
<IFRANGE>	Specifies the range of VLAN interfaces for which the supplicant status is shown.
`vlan` *<VLAN-ID>*	Specifies a VLAN interface for which the supplicant status is shown.

Usage

- Physical Address Extension (PAE) state:
  - **Initialize**—Authentication is yet to start for the PAE.
  - **Authenticating**—Authentication is in-progress for the PAE.
  - **Authenticated**—Authentication is successful for the PAE.
  - **Held**—Authentication has failed for the PAE and no further authentication attempts will be made till the held period expires.
  - **Unauthenticated**—Authentication has failed for the PAE and no further authentication attempts will be made.
  - **Logoff**—The PAE no longer wishes to be authenticated.
- Status and forwarding state (FS):
  - **Open**—The PAE did not find a 802.1X authenticator within the discovery period. FS: Forwarding
  - **Blocked**—The PAE is currently authenticating and the port is operating in start-mode start-closed or has failed authentication and the port is operating in fail-mode fail-closed. FS: Blocked
  - **Disabled**—The port to which the interface is attached is not ready or has an invalid configuration. FS: Blocked
  - **Secured**—The PAE is authenticated. FS: Forwarding
  - **Start-Open**—The PAE is currently authenticating and the port is operating in start-mode start-open. FS: Forwarding
  - **Fail-Open**—The PAE has failed authentication and the port is operating in fail-mode fail-open. FS: Forwarding

Examples

Showing the 802.1X supplicant status on all enabled interfaces:

```
switch# show aaa authentication port-access dot1x supplicant status

802.1X Supplicant Status

 Interface  Policy         PAE State        Authenticator      EAP Method  Status
 -------- --------------- ---------------- ------------------ ----------- --------
--
 1/1/1     CX_Policy_01    Authenticated    38:21:c7:59:ad:27  EAP-TLS     Secured
 1/1/2     CX_Policy_02    Authenticating   38:21:c7:59:ad:28  EAP-MD5     Blocked
 1/1/3     CX_Policy_01    Unauthenticated  38:21:c7:59:ad:29  EAP-TLS     Fail-
Open
 1/1/4     CX_Policy_03    Unauthenticated  --                 --          Open
```

Showing the 802.1X supplicant status on a specific interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface
1/1/1

802.1X Supplicant Status

 Interface  Policy          PAE State        Authenticator      EAP Method  Status
 ---------- --------------- ---------------- ------------------ ----------- -------
---
 1/1/1      CX_Policy_01    Authenticated    38:21:c7:59:ad:27  EAP-TLS
Secured
```

Showing the message when the feature is not enabled on any interface of the system:

```
switch# show aaa authentication port-access dot1x supplicant status
802.1X supplicant is not configured.
```

Showing the message when the feature is not enabled on the interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface
1/1/1
802.1X supplicant is not configured.
```

When an interface range is entered, this message is displayed only if the 802.1X supplicant is disabled either globally or on each interface specified in the user input.

Showing the message when there are no 802.1X supplicants on the system:

```
switch# show aaa authentication port-access dot1x supplicant status
No 802.1X supplicants found.
```

Showing the message when there are no 802.1X supplicants on the interface:

```
switch# show aaa authentication port-access dot1x supplicant status interface
1/1/1
No 802.1X supplicants found.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

start-mode

```
start-mode[start-closed | start-open]
no start-mode [start-closed | start-open]
```

Description

Configures the forwarding behavior of the interface on the data-plane when the authentication is in-progress during the first run of the supplicant. Default: start-open.

The **no** form of the command resets it to the default.

Examples

Configuring the start mode as start-closed:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# start-mode start-closed
```

Resetting the start mode to the default value in the system:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# no start-mode

OR

switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)#policy CX_Policy
switch(config-dot1x-supp-policy)# no start-mode start-closed
```

When the value does not match the currently configured non-default value for start-mode:

```
switch(config)# aaa authentication port-access dot1x supplicant
switch(config-dot1x-supp)# policy CX_Policy
switch(config-dot1x-supp-policy)# start-mode start-closed
switch(config-dot1x-supp-policy)# no start-mode start-open
The input value does not match the currently configured value.
```

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

Command History

Release	Modification
10.09	Command introduced.

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-dot1x-supp`
	`config-dot1x-supp-policy`
		Administrators or local user group members with execution rights for this command.

Chapter 67
Port access cached-critical role commands

aaa authentication port-access cached-critical-role (global)

```
aaa authentication port-access cached-critical-role
   enable
   disable
   cache-timeout <HOURS>
   cache-replace-mode {fifo|none}
   no ...
   persistent-storage {enable |write-interval <INTERVAL>}
```

Description

Enters the cached-critical role context (shown in the switch prompt as config-aaa-ccr). The cached-critical role allows the authorization of authenticated clients with the previously applied roles when the RADIUS server is unreachable.

By default, the cached-critical role is disabled at the global level. When the cached-critical user role is enabled, the MAC address of clients and their applied roles are cached in the following cases:

- During the client log-off.
- When a client fails to reach the server during reauthentication.
- All the RADIUS servers in the server group are not reachable. In this case, the details of the clients authenticated with the server group are cached.

When the RADIUS server is unreachable, the cached-critical role is applied as a special role. The cached-critical role can be applied only on authentication-enabled ports.

If a server group configured on a port becomes unreachable, caching is not performed for individual clients dependent that group.

By enabling the **persistent-storage** configuration, the cached-critical role support for the clients will be available across switch reboots. With this configuration enabled, the client information is cached in the persistent memory of the switch. The information stored in the persistent storage is updated periodically and the interval between the updates is configurable using the **write-interval** CLI option, with a default interval of 3600 seconds. The update to the persistent storage is only done if there is a difference in the client information since the last write.

The **no** form of the command disables the cached-critical role. This is the default.

- The **persistent-storage** option must be enabled *before* the clients are onboarded. If the configuration is disabled after a client has onboarded, the feature might not work across a reboot for the clients which are onboarded with DUR/RADIUS roles.
- If the cached-critical user role needs to be modified to add a captive portal profile, use the **port-access clear cached-client role <ROLE>** command to clear the cached clients on the role before it is modified.
- Enabling **persistent-storage** on the switch might reduce the lifespan of persistent memory.

Parameter	Description
`enable`	Enables the cached-critical role on the authentication-enabled ports.
`disable`	Disables the cached-critical role. (Default)
`cache-timeout <HOURS>`	Specifies the timeout period for the client details to be cached in the switch. A timer runs for every 30 minutes interval to check whether the client is valid to stay cached. On a timeout, the cached entry is removed from the switch within the buffer time of 30 minutes. Default: 96 hours. Range: 1 to 168 hours.
`cache-replace-mode {fifo|none}`	Sets the cache replacement mode. ■ **fifo**: Sets the cache replace mode to **fifo** (First in, first out). If the number of cached clients in the system exceeds the limit of 1024, the oldest cache entry of the client is replaced with a new entry. ■ **none**: Sets the cache replace mode to **none**. If the number of cached clients in the system exceeds the limit of 1024, the new client details will not be cached. This is the default.
`no ...`	Negates any existing parameter.
`persistent-storage {enable |write-interval <900-86400>}`	Configures the persistent storage for cached clients. ■ **enable**: Enables persistent storage for the cached clients. ■ **write-interval**: Configures the interval between consecutive writes to persistent storage in seconds. Range: 900 to 86400 seconds. Default: 3600 seconds.

Examples

Enabling the cached-critical-role at the global level with a cache timeout period of **72** hours and cache replace mode as **fifo**:

```
switch(config)# aaa authentication port-access cached-critical-role
switch(config-aaa-ccr)# enable
switch(config-aaa-ccr)# cache-timeout 72
switch(config-aaa-ccr)# cache-replace-mode fifo
```

Disabling the cached-critical role at the global level:

```
switch(config)# aaa authentication port-access cached-critical-role
switch(config-aaa-ccr)# disable
```

Enabling and configuring persistent storage:

```
switch(config)#aaa authentication port-access cached-critical-role
switch(config-aaa-ccr)# persistent-storage
switch(config-aaa-ccr-ps)# enable
switch(config-aaa-ccr-ps)# write-interval 7200
```

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	The **persistent-storage** parameter is added. Command introduced on the 6000 and 6100.

Command Information

Platforms	Command context	Authority
6000 6100	`config` `config-aaa-ccr`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access cached-critical-role (per interface)

```
aaa authentication port-access cached-critical-role
no aaa authentication port-access cached-critical-role
```

Description

Enables or disables cached-critical role feature on a specific interface. The cached-critical role allows the authenticated client to be authorized with the previously applied roles when the RADIUS server is unreachable.

By default, the cached-critical role feature is enabled at the port level if the cached-critical role is already enabled globally. This command can be used to configure the cached-user role on the specific ports where the caching is needed.

The **no** form of the command disables the cached-critical role on a specific interface.

Examples

Enabling the cached-critical role on the specific port:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access cached-critical-role
```

Disabling the cached-critical role on the specific port:

```
switch(config)# interface 1/1/1
switch(config-if)# no aaa authentication port-access cached-critical-role
```

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 6000 and 6100.

Command Information

Platforms	Command context	Authority
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

port-access clear cached-client

`port-access clear cached-client [all | mac <MACADDR> | role <ROLENAME>]`

Description

Clears all the cached clients or clears cached clients based on the MAC address or role name.

Parameter	Description
`all`	Clears all the cached clients.
`mac <MACADDR>`	Clears cached clients based on the MAC address.
`role <ROLENAME>`	Clears cached clients based on the role.

Examples

Clearing all the cached clients:

```
switch# port-access clear cached-client all
```

Clearing the cached clients based on the MAC address:

```
switch# port-access clear cached-client mac 00:0a:0b:0c:0d:0e
```

Clearing the cached clients based on the role:

```
switch# port-access clear cached-client ap_role
```

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 6000 and 6100.

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show port-access cached-clients

`show port-access cached-clients [mac <MAC-ADDRESS>][role <ROLE-NAME>]`

Description

Shows summarized information of all cached port-access clients on the system. The output can be filtered by MAC address or role.

The role name is not displayed for clients that use a RADIUS role without a base role.

Parameter	Description
<MAC-ADDRESS>	Specifies the MAC address of the client.
<ROLE-NAME>	Specifies the role of the client.

Examples

Showing summarized information for all cached port-access clients on the system:

```
switch# show port-access cached-clients
Port Access Cached-Clients
RADIUS overridden user roles are suffixed with '*'
------------------------------------------------------------------------
MAC-Address        Role              Cached-Duration
------------------------------------------------------------------------
00:50:56:bd:04:c8  ap-role           3 Days, 22 Hours, 33 Minutes, 44 Seconds
00:50:56:bd:32:07                    1 Day, 1 Hour, 1 Minute, 1 Second
00:50:56:bd:32:08                    12 Hours, 34 Minutes, 56 Seconds
00:50:56:cd:32:09  ap-role           12 Hours, 56 Seconds
00:50:56:bd:50:43  employee          12 Hours
00:50:56:bd:50:45  printer           34 Minutes
08:97:34:ad:e4:00  role_01_Student   56 Seconds
10:2f:09:89:00:35  A-Role*           54 Minutes, 26 Seconds
```

Showing information for a specific client based on the MAC address:

```
switch# show port-access cached-clients clients mac 00:50:57:bd:32:09
Port Access Cached-Clients
RADIUS overridden user roles are suffixed with '*'
--------------------------------------------------------------------------
MAC-Address        Role              Cached-Duration
--------------------------------------------------------------------------
00:50:56:bd:32:08                    12 Hours, 34 Minutes, 56 Seconds
```

Showing information for a specific client based on the role:

```
switch# show port-access cached-clients role
ROLE  The role name.
switch# show port-access cached-clients role intern
No port-access cached-clients found
switch# show port-access cached-clients role ap-role
Port Access Cached-Clients
RADIUS overridden user roles are suffixed with '*'
--------------------------------------------------------------------------
MAC-Address        Role              Cached-Duration
--------------------------------------------------------------------------
00:50:56:bd:04:c8  ap-role           3 Days, 22 Hours, 33 Minutes, 44 Seconds
00:50:56:cd:32:09  ap-role           12 Hours, 56 Seconds
```

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 output modified to be suffixed with * for RADIUS overridden user roles. The role name will not displayed for clients that use a RADIUS role without a base role.
10.11.1000	Command introduced on the 6000 and 6100.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access cached-critical-role info

```
show port-access cached-critical-role info
```

Description

Shows summarized information of port-access cached-critical role configuration.

Examples

Showing summarized information of the cached-critical role configuration with the status of cached-critical role **Disabled**:

```
switch# show port-access cached-critical-role info

Port Access Cached-Critical-Role
================================

  Cached-Critical-Role Status         : Disabled
  Cache-Timeout                       : 96 Hours
  Cache Replace Mode                  : None
  Cached-Critical-Role Disabled Ports :
  Persistent Storage Status           : Disabled
  Persistent Storage Write Interval   : 900 Seconds
  Last Write To Persistent Storage    : N/A
```

Showing summarized information of the cached-critical role configuration with the status of cached-critical role **Enabled**:

```
switch# show port-access cached-critical-role info

Port Access Cached-Critical-Role
================================

  Cached-Critical-Role Status         : Enabled
  Cache-Timeout                       : 100 Hours
  Cache Replace Mode                  : FIFO
  Cached-Critical-Role Disabled Ports : 1/1/1-1/1/5,1/1/10
  Persistent Storage Status           : Enabled
  Persistent Storage Write Interval   : 7200 Seconds
  Last Write To Persistent Storage    : Mon Aug 08 04:40:49 UTC 2022
```

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	The output is updated to display persistent storage related information. Command introduced on the 6000 and 6100.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 authentication port-access allow-lldp-auth

```
aaa authentication port-access allow-lldp-auth [mac chassis-mac|source-mac]
no aaa authentication port-access allow-lldp-auth [mac chassis-mac|source-mac]
```

Description

This command is an extension of **aaa authentication port-access allow-lldp-auth**.

By default, authentication on chassis-mac is allowed via LLDP packets which are received on the port. Use the Chassis MAC shown in the LLDP TLV or the source MAC in the LLDP frame.

Use the **no** version of this command to prevent authentication using LLDP packets received on the port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts along with the following commands:

```
interface lag 1
        aaa authentication port access
allow-lldp-bpdu
        aaa authentiction port access
allow-lldp-auth mac source-mac
```

Parameter	Description
mac	(Optional) Specify the LLDP authentication-mac type.
chassis-mac	Configure LLDP authentication-mac type as a chassis MAC address. This is the default value.
source-mac	Configure LLDP authentication-mac type as an interface MAC address

Examples

Configuring authentication via LLDP packets:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-lldp-auth
switch(config)# interface lag 1
switch(config-lag-if)# aaa authentication port-access allow-lldp-auth
```

Enabling/disabling authentication via LLDP BPDU packets:

```
switch(config-if)# aaa authentication port-access
allow-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
allow)
```

```
switch(config-if)# no aaa authentication port-access
allow-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
allow)
switch(config-if)# aaa authentication port-access allow-lldp-auth
switch(config-if)# no aaa authentication port-access allow-lldp-auth

switch(config-if)# aaa authentication port-access
block-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
block)
switch(config-if)# no aaa authentication port-access
block-lldp-auth Allow or block authentication on LLDP BPDU. (Default:
block)
```

Configuring the MAC to use for authentication:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-lldp-auth mac source-mac
switch(config-if)# aaa authentication port-access allow-lldp-auth mac chassis-mac
```

```
switch(config-if)# aaa authentication port-access allow-lldp-auth
mac    Configure the MAC to use for LLDP based authentication (Default:
chassismac)

switch(config-if)# aaa authentication port-access allow-lldp-auth mac
chassis-mac   Use the chassis MAC in LLDP TLV.
source-mac       Use the source MAC in the LLDP frame.
```

Disabling authentication via LLDP packets based on MAC source:

```
switch(config-if)# no aaa authentication port-access allow-lldp-auth mac
chassis-mac     Use the chassis MAC in LLDP TLV.
source-mac      Use the source MAC in the LLDP frame.
```

Disabling authentication via LLDP packets on a LAG port:

```
switch (config) interface lag 1
switch(config-lag if)# no aaa authentication port-access allow-lldp-auth
```

When a client such as dual-homed access points and switches, connects to the switch over multiple physical interfaces and use LLDP packets to onboard, it is recommended to use LLDP authentication MAC as the source MAC on the interfaces. This prevents the switch from learning the client MAC from the chassis MAC in the LLDP TLV (default), similarly to the LLDP BPDUs received on all interfaces connected to the same device. If the MAC learned is the chassis MAC, it will cause the switch to treat the client as moving between the different interfaces each time a LLDP BPDU is received on an interface. Additionally, using a different LLDP authentication MAC type on interfaces connecting to the same device may lead to undesired behavior.

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.09	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-mode

```
aaa authentication port-access auth-mode {client-mode | device-mode | multi-domain}
```

Description

Configures the authentication mode for the port. By default, client mode is enabled. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

Parameter	Description
`client-mode`	Selects client mode. In this mode, all clients connecting to the port are sent for authentication. The maximum number of clients allowed to connect to the port is limited by the client limit value configured with the **aaa authentication port-access client-limit** command.
`device-mode`	Selects device mode. In this mode, only the first client connecting to the port is sent for authentication. Once this client is authenticated, the port is considered as open and all subsequent clients trying to connect on that port are not sent for authentication.
`multi-domain`	Selects multidomain mode. In this mode only one voice device is allowed to be authenticated in addition to the configured data devices on a port. By default only one data device is allowed to be authenticated on the multidomain mode along with one voice device. You can configure the maximum number of data devices allowed with the **aaa authentication port-access client-limit multi-domain** command. If a second voice device or a data device greater than the configured data client limit onboards, a violation is triggered. You must configure a voice VLAN for IP phones to onboard a voice device in the multidomain authentication mode. To authorize a voice device, you must perform one of the following: ▪ Configure the AAA server to send the **Aruba-Device-Traffic-Class** Aruba VSA with value **1**. ▪ Configure the **device-traffic-class** parameter in the role to be applied to indicate a voice device. Without this VSA value or the device type in the role, the switch considers the voice device as a data device.

Parameter	Description
	NOTE: This parameter is not supported when the command is issued from the LAG (**config-lag-if**) context.

Examples

Configuring device mode authentication for interface 1/1/1:

```
switch(config)# interface  1/1/1
switch(config-if)# aaa authentication port-access auth-mode device-mode
```

Configuring device mode authentication for a LAG port:

```
switch(config)# interface lag 1
switch(config-lag if)# aaa authentication port-access auth-mode device-mode
```

Configuring multidomain mode authentication for a port:

```
switch(config)# interface  1/1/1
switch(config-if)# aaa authentication port-access auth-mode multi-domain
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.08	Added **multi-domain** parameter
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-precedence

```
aaa authentication port-access auth-precedence [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-precedence [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-precedence
```

Description

Configures the per port authentication precedence using the space separator.

By default, 802.1X authentication (**dot1x**) takes a higher precedence than MAC authentication (**mac-auth**).

The **no** form of the command resets the port access authentication precedence to the default, 802.1X authentication followed by MAC authentication.

Parameter	Description
`dot1x mac-auth`	Specifies that the port access authentication precedence is 802.1X authentication followed by MAC authentication.
`mac-auth dot1x`	Specifies that the port access authentication precedence is MAC authentication followed by 802.1X authentication.

Examples

Configuring MAC authentication precedence on a port:

```
switch(config-if)# aaa authentication port-access auth-precedence mac-auth dot1x
```

Resetting the authentication precedence to the default value:

```
switch(config-if)# no aaa authentication port-access auth-precedence mac-auth
dot1x
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-priority

```
aaa authentication port-access auth-priority [dot1x mac-auth | mac-auth dot1x]
no aaa authentication port-access auth-priority [dot1x mac-auth | mac-auth  dot1x]
no aaa authentication port-access auth-priority
```

Description

Configures the authentication priority using the space separator to specific interface.

Default **auth-priority** with concurrent onboarding is 802.1X followed by MAC authentication. With authentication precedence, the default **auth-priority** follows the **auth-precedence** order.

The **no** form of the command resets the port access authentication priority to the default, is same as the configured **auth-precedence** order.

The authentication priority is useful in deployments where clients such as wireless access points (APs), IT-compliant-laptops or phones, or laptops without pre-loaded supplicant software must download the supplicant software or firmware patches before attempting 802.1X authentication. In such cases, configure the MAC authentication as the primary authentication method followed by 802.1X for the authentication order. Meanwhile, configure 802.1X as the primary authentication priority and MAC authentication as secondary to enforce access based on 802.1X. Thus the client (or end access device) will initially be authenticated by MAC authentication with the access required to onboard and install the software or patches, and subsequently attempt the 802.1X authentication.

Reauthentication will be triggered for all high priority methods and not just the final successful authentication method.

Parameter	Description
`dot1x mac-auth`	Specifies that the port access authentication precedence is 802.1X authentication followed by MAC authentication.
`mac-auth dot1x`	Specifies that the port access authentication precedence is MAC authentication followed by 802.1X authentication.

Examples

Configuring MAC authentication priority on a port:

```
switch(config-if)# aaa authentication port-access auth-priority mac-auth dot1x
```

Resetting the authentication priority to the default value:

```
switch(config-if)# no aaa authentication port-access auth-priority mac-auth dot1x
switch(config-if)# no aaa authentication port-access auth-priority
```

Sample configuration:

```
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    aaa authentication port-access auth-precedence mac-auth dot1x
    aaa authentication port-access auth-priority dot1x mac-auth
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access auth-role

```
aaa authentication port-access [critical-role|preauth-role|reject-role|
   auth-role|critical-voice-role] <ROLE-NAME>
no aaa authentication port-access [critical-role|preauth-role|reject-role|
   auth-role|critical-voice-role]
```

Description

Configures the role to assign to the clients depending on the client authentication state.

The **no** form of the command disassociates the roles that you assign to clients based on the authentication state.

Parameter	Description
`critical-role`	Specifies the role that is applied when the RADIUS server is unreachable for authentication or when there is a request timeout.
`preauth-role`	Specifies the role that is applied when authentication is still in progress.
`reject-role`	Specifies the role that is applied when authentication has failed.
`auth-role`	Specifies the role that is applied to authenticated clients when a specific role is not assigned in the RADIUS server.
`critical-voice-role`	Specifies the role for a voice client when the RADIUS server is unreachable for authentication during reauthentication period. This is applicable when multidomain authentication mode is enabled with the **aaa authentication port-access auth-mode** command.
<ROLE-NAME>	Specifies the role name.

Examples

Configuring critical role for clients:

```
switch(config-if)# aaa authentication port-access critical-role role1
```

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

Command History

Release	Modification
10.08	Added **critical-voice-role** parameter
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access client-auto-log-off final-authentication-failure

```
aaa authentication port-access client-auto-log-off final-authentication-failure
no aaa authentication port-access client-auto-log-off final-authentication-failure
```

Description

Use this command to automatically remove a client when authentication fails due to any reason except **server-reject** or **server-timeout**. This feature is disabled by default.

The **no** form of this command disables this feature if it has been previously enabled.

Automatic client log-off is not supported on Layer-3 interfaces.

Examples

Configuring the client-auto-log-off feature on interface 1/1/1:

```
switch(config)# interface  1/1/1
switch(config-if)# aaa authentication port-access client-auto-log-off final-
authentication-failure
```

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

Command History

Release	Modification
10.08.1090	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access client-limit

```
aaa authentication port-access client-limit <CLIENTS>
no aaa authentication port-access client-limit
```

Description

Configures the maximum number of clients that can simultaneously connect to a port. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

The **no** form of this command resets the number of clients to the default.

Parameter	Description
<CLIENTS>	Specifies the maximum number of clients. Default: 1. Range: 1 to 32 (6000, 6100, 4100i).

Examples

Configuring the client limit for on port **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access client-limit 25
```

Configuring the client limit for on a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# aaa authentication port-access client-limit 25
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access client-limit multi-domain

```
aaa authentication port-access client-limit multi-domain <DATA-CLIENT-LIMIT>
```

Description

Configures the data client limit on the multidomain enabled interface. By default, the data client limit on a multidomain enabled interface is **1**, and the maximum number of data clients supported on a multidomain enabled port is **5**.

Parameter	Description
<DATA-CLIENT-LIMIT>	Specifies the maximum data client limit on the multidomain enabled interface. Range: **1** to **5**.

Examples

Configuring data client limit of **4** on the multidomain enabled interface **1/1/4**:

```
switch(config)# interface  1/1/1
switch(config-if)# aaa authentication port-access client-limit multi-domain 4
```

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

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access radius-override

```
aaa authentication port-access radius-override {enable | disable}
no aaa authentication port-access radius-override {enable | disable}
```

Description

Enables or disables **radius-override** support at the interface context. When **radius-override** support is enabled, a new RADIUS overridden role is created with a combination of LUR/DUR along with RADIUS attributes for the corresponding client-role attributes such as VLANs, captive portal URL, and downloadable gateway role. When the RADIUS override support is disabled, then only the user-roles get applied to the client.

The **no** form of this command disables the support for **radius-override**.

(DUR (Downloadable User Role) is not available on the 6000, 6100 Switch Series).

The **radius-override** support is applicable only for Auth-role.

Usage

The following table describes the access-response for the combination of roles with **radius-override** enabled and disabled:

Combination of roles in Access-Accept	Action with *radius-override* disabled	Action with *radius-override* enabled
Local User Role and RADIUS attributes	Local User Role is applied	New RADIUS Overridden role with Local User Role and RADIUS attributes is created and applied
Downloadable User Role and RADIUS attributes	Downloadable User Role is applied	New RADIUS Overridden role with Downloadable User Role and RADIUS attribute is created and applied
Local User Role and Downloadable User Role	Local User Role is applied	Local User Role is applied
Local User Role, Downloadable User Role, and RADIUS attributes	Local User Role is applied	New RADIUS Overridden role with Local User Role and RADIUS attributes is created and applied

Examples

Enabling radius-override support:

```
switch(config-if)# aaa authentication port-access radius-override enable
```

```
switch(config-if)# no aaa authentication port-access radius-override disable
```

Disabling radius-override support:

```
switch(config-if)# aaa authentication port-access radius-override disable
```

```
switch(config-if)# no aaa authentication port-access radius-override enable
```

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

Command History

Release	Modification
10.09.1000	Added captive portal support on the 4100i, 6000, 6100
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

port-access allow-flood-traffic

```
port-access allow-flood-traffic {enable | disable}
```

Description

Enables or disables transmission of flood traffic, such as broadcast, multicast, and unknown unicast messages through a security enabled port on which no client has been authenticated. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts. By default, transmission of flood traffic is disabled.

Usage

This command can be used to allow Wake-on-LAN packets on security enabled ports, before a client is authenticated.

Examples

Enabling flood traffic on a port on interface 1/1/1:

```
switch(config)# interface  1/1/1
switch(config-if)# port-access allow-flood-traffic
```

Enabling flood traffic on a port on a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# port-access allow-flood-traffic
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

port-access client-move

`port-access client-move {enable | disable | secure}`

Description

When client move is enabled (the default), a port access client can move to other port access-enabled interfaces, at which time they will be re-authenticated on the new interface.

When client move is disabled, a client cannot move to other port access-enabled interfaces.

An authenticated client will be moved immediately if the new port to which the client will move has a pre-auth role configured, even when client move is enabled as secure.

Parameter	Description
`enable`	Enables this feature so port access clients can move to other port access-enabled interfaces.
`disable`	Disables this feature so port access clients cannot move to other port access-enabled interfaces.
`secure`	Use this configuration setting to stop a potential attacker from denying a genuine client access by spoofing the client's MAC on a different port-access enabled port of the switch. An authenticated client will be moved immediately if the new port to which the client moved has a pre-authentication role configured, even when client-move is enabled as secure. **NOTE:** Secure client move is enabled by default.

Examples

Enabling client move:

```
switch(config)# port-access client-move enable
```

Enabling secure client move:

```
switch(config)# port-access client-move enable secure
```

Disabling client move:

```
switch(config)# port-access client-move disable
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

port-access event-log client

```
port-access event-log client
no port-access event-log client
```

Description

Enables port access informational event logs for the client. These event logs help with client telemetry on a remote management station such as Aruba Central. By default, these informational event logs are disabled.

Starting with AOS-CX 10.10, the event IDs 10510 and 10511 are logged when the port access informational event log configuration is enabled.

The **no** form of the command disables port access informational event logs for the client.

Example

Enabling port access event log:

```
switch(config)# port-access event-log client
```

Disabling port access event log:

```
switch(config)# no port-access event-log client
```

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
6000 6100	config	Administrators or local user group members with execution rights for this command.

port-access fallback-role

```
port-access fallback-role <ROLE-NAME>
no port-access fallback-role <ROLE-NAME>
```

Description

Configures the fallback role to assign to the clients onboarding on a port. This role is applied only when no derived role is applied to the clients.

The **no** form of the command resets the fallback role.

Parameter	Description
<ROLE-NAME>	Specifies the fallback role name. The maximum number of characters supported is 64.

Usage

Following are the conditions for the fallback role to be applied on onboarding devices:

- The device profile local MAC match feature with block-until-profile-applied mode is configured.
- Device profile along with AAA is configured but no match was found for the device profile client.
- AAA method with no reject or critical role is configured, and the connection to RADIUS server failed.
- 802.1X authentication is enabled on the port, but the supplicant of the device timed out to respond to the authentication request.

Example

Configuring fallback role for a port:

```
switch(config)# interface  1/1/3
switch(config-if)# port-access fallback-role fallback01
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

port-access log-off client

```
port-access log-off client mac <MAC-ADDRESS>
port-access log-off client interface <INTERFACE-NAME>
port-access log-off client role <ROLE-NAME>
```

Description

Logs off the client connected to a port access-enabled interface.

Parameter	Description
<MAC-ADDRESS>	Specifies the client MAC address.
<INTERFACE-NAME>	Specifies the client interface.
<ROLE-NAME>	Specifies the client MAC address.

Example

Logging a client off from the switch, specifying the MAC address:

```
switch# port-access log-off client mac 00:50:56:bd:04:2d
```

Logging a client off from the switch, specifying the interface:

```
switch# port-access log-off client interface 1/1/1
```

Logging a client off from the switch, specifying the role:

```
switch# port-access log-off client role r1
```

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
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

port-access onboarding-method precedence

```
port-access onboarding-method precedence [aaa device-profile | device-profile aaa]
no port-access onboarding-method precedence [aaa device-profile | device-profile aaa]
```

Description

Configures the precedence for the method to be used to authenticate onboarding devices for each interface.

The **no** form of the command resets the authentication method precedence to the default precedence of AAA followed by device profile.

AAA includes the 802.1X and MAC authentication methods whose precedence can be configured using the **aaa authentication port-access auth-precedence** command. Here, the default precedence is 802.1X authentication.

For example, if you configure AAA (both 802.1X and MAC) authentication methods and device profile on a port, by default, the authentication precedence would be 802.1X, then MAC, and lastly device profile.

aaa in the parameters refers to the authentication precedence configured using the **aaa authentication port-access auth-precedence** command.

Parameter	Description
`aaa device-profile`	Specifies that the precedence for per port onboarding authentication method is AAA followed by device profile.
`device-profile aaa`	Specifies that the precedence for per port onboarding authentication method is device profile followed by AAA.

Examples

Configuring AAA method precedence on a port:

```
switch(config)# interface  1/1/1
switch(config-if)# port-access onboarding-method precedence device-profile aaa
```

Resetting the authentication method precedence:

```
switch(config)# interface  1/1/1
switch(config-if)# no port-access onboarding-method precedence device-profile aaa
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

port-access onboarding-method concurrent

```
port-access onboarding-method concurrent <enable | disable>
```

Description

Configures all methods to start concurrently for faster onboarding process. If authentication priority is not configured when enabling concurrent onboarding, the priority will be 802.1X followed by **mac-auth** and **device-profile**.

Default priority for concurrent onboarding is 802.1X followed by **mac-auth** and **device-profile**.

When enabling concurrent onboarding on the port, existing clients will be de-authenticated and freshly onboarded concurrently.

When concurrent onboarding is enabled, then auth-precedence will be ignored.

If concurrent onboarding is configured, the client will stay in pre-auth role till it gets succeeded by one authentication method or gets failed by all the authentication methods.

When the authentication method with the highest priority fails, the profile of the next successful authentication method is applied.

If all methods fail, the reject or critical role is applied based on the 802.1X authentication failure reason and continues to reauthenticate with the 802.1X method.

Reauthentication will be triggered for all high priority methods and not just the final successful authentication method.

Some RADIUS server may block the client when it receives two requests, **mac-auth** and 802.1X, from the same client at the same time. This is because the RADIUS server allows only one authentication request. In such cases, concurrent onboarding is not feasible. To prevent such scenarios, configure **auth-precedence** with **auth-priority**.

Parameter	Description
enable	Enable clients to be onboarded concurrently.
disable	Disable clients to be onboarded concurrently.

Examples

Enabling concurrent onboarding on a port:

```
switch(config)# interface  1/1/1
switch(config-if)# port-access onboarding-method concurrent enable
```

Disabling concurrent onboarding on a port:

```
switch(config)# interface  1/1/1
switch(config-if)# port-access onboarding-method concurrent disable
```

Sample configuration:

```
interface 1/1/1
    no shutdown
    no routing
    vlan access 999
    !aaa authentication port-access auth-precedence mac-auth dot1x
    port-access onboarding-method concurrent enable
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

port-access reauthenticate interface

`port-access reauthenticate interface <INTERFACE-NAME>`

Description

Forcefully reauthenticates all clients connected to an interface.

Clients that are in the **HELD** state are ignored.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.

Examples

Configuring reauthentication of all clients on a port:

```
switch# port-access reauthenticate interface 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
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show aaa authentication port-access interface client-status

```
show aaa authentication port-access interface {all | <IFRANGE>}
client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about the status of the role applied on ports. RADIUS overridden user roles are suffixed with *. The role name is not displayed for clients that do not use local, downloaded, or RADIUS overridden role.

Parameter	Description
`all`	Specifies all interfaces.
<IFRANGE>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing information about a client:

```
switch# show aaa authentication port-access interface all client-status
Port Access Client Status Details
RADIUS overridden user roles are suffixed with '*'
Client 00:50:56:96:93:d6, John Doe
============================

Session Details
---------------
Port         : 1/1/13
Session Time : 30s
IPv4 Address : 10.0.0.1
IPv6 Address :


Authentication Details
```

```
----------------------
Status          : dot1x Authenticated
Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
Auth History    : dot1x    - Authenticated, 5s ago
mac-auth - Unauthenticated, Server-Reject, 10s ago
mac-auth - Unauthenticated, Server-Reject, 15s ago
dot1x    - Unauthenticated, Server-Timeout, 15s ago
dot1x    - Attempted, 20s ago


Authorization Details
----------------------
Role   : Employee*
Status : Applied


Client 00:50:56:96:50:28
============================
Session Details
---------------
Port         : 1/1/14
Session Time : 10s
IPv4 Address : 10.0.0.2
IPv6 Address :


Authentication Details
----------------------
Status          : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History    : dot1x    - Unauthenticated, Server-Reject, 5s ago
mac-auth - Authenticated, 10s ago


Authorization Details
----------------------
Status : Applied
```

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 output modified to be suffixed with * for RADIUS overridden user roles. The role name will not be displayed for clients that do not use local, downloaded, or RADIUS overridden role.
10.08	Command output updated to display multidomain mode information
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access clients

`show port-access clients [dhcp-info|ubt|vxlan] [interface <INTERFACE-NAME>] [mac <MAC-ADDRESS>]`

Description

Shows summarized active port access client information.

The **User-Role** column in the output will not display any value for clients not using local, downloaded or RADIUS overridden role. When an explicit client name is not available, only the MAC address of the client will be displayed.

The VLANs in the output display the tags, **u, t**, and **multi** to indicate untagged VLAN, single tagged VLAN, and multiple VLANs respectively.

Parameter	Description
dhcp	Shows DHCP information of port access clients. **NOTE:** To view the DHCP information of port access clients, either client IP tracker or DHCP snooping must be enabled. If client IP tracker is enabled, then the command does not display the lease time. This command does not display information about tagged VLAN.
ubt	Shows port access information about UBT clients. **NOTE:** The output displays information only about untagged VLAN.
vxlan	Shows port access information about VXLAN clients. **NOTE:** The output displays information about both tagged and untagged VLAN without the tags, **u** and **t**.
<INTERFACE-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing information about a specific client:

```
switch# show port-access clients mac 00:50:56:bd:50:43
Port Access Clients
RADIUS overridden user roles are suffixed with '*'
```

```
Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile,m
Multi-Domain

Mode: c Client-Mode, d Device-Mode, , m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

------------------------------------------------------------------------------
---------------------------
Port     Client-Name             IPv4-Address    User-Role
  VLAN            Flags
------------------------------------------------------------------------------
---------------------------
1/1/5    00:50:56:bd:50:43                       reject-role, reject
  (u)1234,(t)1000 1x|c|-|s
```

Showing information for clients on a particular interface:

```
switch# show port-access clients interface 1/1/5
Port Access Clients
RADIUS overridden user roles are suffixed with '*'

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile

Mode: c Client-Mode, d Device-Mode,  m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

------------------------------------------------------------------------------
---------------------------
Port     Client-Name             IPv4-Address    User-Role
  VLAN            Flags
------------------------------------------------------------------------------
---------------------------
1/1/5    00:50:56:bd:32:07                       reject-role, reject
  (u)1234,(t)1000 1x|c|-|s
1/1/5    test                                    critical-..., critical
  (u)56           1x|c|-|f
1/1/9    00:50:56:bd:50:c7                       rp-role
                 rp|p|-|s
```

Showing DHCP information of port access clients:

```
switch# show port-access clients dhcp-info
Port Access Clients
------------------------------------------------------------------------------
--------------
Port     Client-Name             IP-Address
VLAN  Lease-Time
```

```
--------------------------------------------------------------------------------
--------------
1/1/1    Camera-1023            10.10.10.10                                  10
  268
1/1/2    CAP-8-G22              aaaa:bbbb:cccc:dddd:eeee:1234:5678:abcd      20
  500
```

Showing port access information about UBT clients:

```
switch# show port-access clients ubt
Port Access Clients
RADIUS overridden user roles are suffixed with '*'

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile

Mode: c Client-Mode, d Device-Mode,m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

--------------------------------------------------------------------------------
-------------------------------------
Port     Client-Name         IPv4-Address    User-Role              Gateway-Role
        UBT           VLAN  Flags
Zone
--------------------------------------------------------------------------------
-------------------------------------
1/1/12   00:50:56:96:93:d6   10.10.10.10     test_role              authenticated
        zone1         10    ma|c|-|s
1/1/10   CAP-8-G22           10.10.10.11     student
authenticated_gate... zone1         9857  1x|c|-|s
```

Showing port access information about VXLAN clients:

```
switch# show port-access clients vxlan
Port Access Clients
RADIUS overridden user roles are suffixed with '*'

Flags: Onboarding-Method|Mode|Device-Type|Status

Onboarding-Method: 1x 802.1X, ma MAC-Auth, ps Port-Security, dp Device-Profile

Mode: c Client-Mode, d Device-Mode, m Multi-Domain

Device-Type: d Data, v Voice

Status: s Success, f Failed, p In-Progress, d Role-Download-Failed

--------------------------------------------------------------------------------
----------------------
Port     Client-Name             IPv4-Address    User-Role
  VLAN  VNI  Flags
--------------------------------------------------------------------------------
----------------------
```

```
1/1/21    00:50:56:96:93:d6       10.10.10.10     student
  5678   2432 ma|c|-|s
1/1/21    user_12@gmail.com                       employee
  9857   4678 1x|c|-|s
```

Command History

Release	Modification
10.12	The following changes were introduced: ■ The **dhcp-info**, **ubt**, and **vxlan** parameters were introduced. ■ Command output modified to display only **Port**, **Client-Name**, **IPv4-Address**, **User-Role**, **VLAN,** and **Flags.**
10.11.1000	Command output updated to display cached-critical role on the 6000 and 6100.
10.08	Command output updated to display multidomain mode information
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access clients detail

`show port-access clients [interface <INTERFACE-NAME>] [mac <MAC-ADDRESS>] detail`

Description

Shows detailed active port access clients information including the VLAN group and VLAN association for each of the authenticated clients. The output can be filtered by interface or MAC address.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing detailed information for clients on a particular interface:

```
switch# show port-access clients interface 1/1/7-1/1/8 detail
Port Access Client Status Details:
```

```
---------------------------------

RADIUS overridden user roles are suffixed with '*'

Client 2c:41:38:7f:35:b9, John Doe
==========================
Session Details
---------------
Port         : 1/1/7
Session Time : 203s
IPv4 Address : 10.10.10.10
IPv6 Address :

Authentication Details
----------------------
Status          : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History    : mac-auth - Authenticated, 5s ago
dot1x    - Unauthenticated, Server-Reject, 10s ago

Authorization Details
---------------------
Status : Applied


RADIUS Attributes
-----------------
User-Name                     : Student
Filter-ID                     : DHCP, WebServices-Student, DataCenter-Student,
RemoteAccess-Student, Printer-Student
Framed-MTU                    : 1500 bytes
Session-Timeout               : 500 seconds
Idle-Timeout                  : 200 seconds
Termination-Action            : RADIUS-Request
Egress-VLAN-ID                : 10(t), 15(t), 20(u)
Egress-VLAN-Name              : VLAN100(t), VLAN200(u)
Tunnel-Type                   : 13
Tunnel-Medium-Type            : 6
Tunnel-Private-Group-ID       : 20
NAS-Filter-Rule               : permit in 17 from any to any
deny in tcp from any to 10.10.10.3/8
Aruba-Captive-Portal-URL      : http://arubanetworks.com/student/captiveportal.php
Aruba-PoE-Priority            : Low
Aruba-Port-Auth-Mode          : client-mode
Aruba-NAS-Filter-Rule         : deny in icmp from 10.10.10.1 to any 27
Aruba-QoS-Trust-Mode          : dscp
Aruba-UBT-Gateway-Role        : gateway_student_role
Aruba-Gateway-Zone            : student_zone
Aruba-STP-Admin-Edge-Port     : false
Aruba-UBT-Gateway-CPPM-Role   : ubt_gateway_cppm_student_role
Aruba-Device-Traffic-Class    : data
Aruba-PVLAN-Port-Type         : secondary
Aruba-PoE-Allocate-By-Method  : class
RADIUS Role Name : RADIUS_115315236
```

Showing information for a particular client MAC address:

```
switch# show port-access clients mac 2c:41:38:7f:35:c8 detail
Port Access Client Status Detail
--------------------------------
RADIUS overridden user roles are suffixed with '*'
```

```
Client 2c:41:38:7f:35:c8, John Doe
==============================

Session Details
---------------
Port         : 1/1/8
Session Time : 33s
IPv4 Address :
IPv6 Address :


VLAN Details
---------------
VLAN Group Name :
VLANs Assigned  : 10,20,30
Access          :
Native Untagged : 10
Alllowed Trunk  : 20,30


Authentication Details
----------------------
Status          : mac-auth Authenticated
Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
Auth History    : mac-auth - Authenticated, 5s ago
dot1x    - Unauthenticated, Server-Timeout, 10s ago


Authorization Details
---------------------
Role   : student
Status : Applied
Role Information:
-----------------
Name  : student
Type  : local
-----------------------------------------------
Reauthentication Period             : 333 secs
Authentication Mode                 : device
Native VLAN                         : 10
Allowed Trunk VLANs                 : 20,30
PoE Allocation method               : usage
PoE Priority                        : low
Captive Portal Profile              : testcpprof_29451201
Policy                              : PERMIT-ALL_87364653


Captive Portal Profile Configuration:
-------------------------------------
Name                            : testcpprof_29451201
Type                            : local
URL                             : http://google.com
URL Hash Key                    : SWNGWyMeYubHPDgVIirpEUwNK5Uf+r1vmhBIncQPw1Y=


Access Policy Details:
----------------------
Policy Name   : PERMIT-ALL_87364653
Policy Type   : Local
Policy Status : Applied
Base Policy   : N/A
ACL Names     : N/A
```

```
SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------------------------
10          dns                            ipv4 permit
20          dhcp                           ipv4 permit


Class Details:
-------------
class ip dns
10 match tcp any any
class ip dhcp
20 match any any any
```

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

Command History

Release	Modification
10.12	The following changes were introduced: ■ Command output modified to display RADIUS attributes for clients not using local, downloaded or RADIUS overridden role. ■ Command output modified to display **Base Policy** and **ACL Names.** ■ Command output modified to display **PoE Allocation method**.
10.08	Added RADIUS overridden role to example
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access clients onboarding-method

`show port-access clients onboarding-method <METHOD>`

Description

Shows active port access client information for the specified onboarding method.

Parameter	Description
<METHOD>	Selects the onboarding method. Available methods: **device-profile**, **dot1x**, **mac-auth**, **port-security**.

Examples

Showing information for clients onboarded using MAC authentication.

```
switch# show port-access clients onboarding-method mac-auth

Port Access Clients

Status codes: device-mode

--------------------------------------------------------------------------------
-
   Port      MAC-Address        Onboarding      Status       Role
                                Method
--------------------------------------------------------------------------------
-
   1/1/6     00:50:56:bd:50:43  mac-auth        Success      auth-role, auth
   1/1/212   00:60:56:bd:50:43  mac-auth        Success      fallback-role,
fallback
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access interface

```
show port-access interface all|<ifrange> status
```

Description

Display the interface status for port-access enabled interfaces. It includes the name of the port, the member interfaces associated with the port along with the security state of the interface.

A port-access interface can be in one of the following states:

1. Blocked: Indicates that the interface is blocked by port-access.
2. Secured: Indicates the interface is secured by port-access.
3. Down: Indicates port-access is not yet operational on the interface

Parameter	Description
all	Display port-access information for all interfaces.
<ifrange>	Display port-access information for the specified interface.

Examples

Showing the port-access status for all interfaces:

```
switch# show port-access interface all status
Port      Interface  Status
--------- ---------- -------
1/1/1     1/1/1      Blocked
lag1      1/1/3      Secured
lag1      1/1/4      Down
```

Showing port-access status for interface 1/1/1:

```
switch# show port-access interface 1/1/1 status
Port      Interface  Status
--------- ---------- -------
1/1/1     1/1/1      Blocked
```

Showing port-access status for LAG 1:

```
switch# show port-access interface lag1 status
Port      Interface  Status
--------- ---------- -------
lag1      1/1/3      Secured
lag1      1/1/4      Down
```

When port-access is not configured on an interface, following message will be displayed:

```
switch# show port-access interface all status
Port-access is not configured
```

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 69
Port access MAC authentication commands

aaa authentication port-access mac-auth

```
aaa authentication port-access mac-auth {enable | disable}
no aaa authentication port-access mac-auth {enable | disable}
```

Description

Enables or disables MAC authentication globally or at the port-level.

Examples

Enabling MAC authentication on all interfaces:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# enable
```

Disabling MAC authentication on all interfaces:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# disable
```

Enabling MAC authentication on an interface:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# enable
```

Disabling MAC authentication on an interface:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# disable
```

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
6000 6100	`config` `config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth addr-format

```
aaa authentication port-access mac-auth addr-format {no-delimiter | single-dash |
     multi-dash |multi-colon | no-delimiter-uppercase | single-dash-uppercase |
     multi-dash-uppercase | multi-colon-uppercase}
no aaa authentication port-access mac-auth addr-format {no-delimiter | single-dash |
       multi-dash |multi-colon | no-delimiter-uppercase | single-dash-uppercase |
       multi-dash-uppercase | multi-colon-uppercase}
```

Description

Configures the MAC address format that the switch must use in the RADIUS request message.

The **no** form of the command resets the MAC address format to the default, **no-delimiter**.

Examples

Setting the MAC address format on the switch:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# addr-format single-dash
```

Resetting the MAC address format on the switch to its default:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# no addr-format
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth auth-method

```
aaa authentication port-access mac-auth auth-method {chap | pap}
no aaa authentication port-access mac-auth auth-method
```

Description

Configures the RADIUS authentication method for MAC authentication.

Following are the MAC authentication methods supported:

- CHAP
- PAP

The PEAP-MSCHAPv2 method of authentication is not supported.

The **no** form of the command resets the authentication method to the default, **chap**.

Examples

Configuring the RADIUS authentication method on the switch:

```
switch# config
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# auth-method pap
```

Resetting the RADIUS authentication method on the switch:

```
switch(config)# no aaa authentication port-access mac-auth auth-method
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth cached-reauth

```
aaa authentication port-access mac-auth cached-reauth
no aaa authentication port-access mac-auth cached-reauth
```

Description

Enables cached reauthentication on a port. Cached reauthentication allows MAC reauthentications to succeed when the RADIUS server is unavailable. Users who are already authenticated, retain their currently assigned RADIUS attributes.

The **no** form of the command disables cached reauthentication.

Examples

Enabling cached reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# cached-reauth
```

Disabling cached reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no cached-reauth
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth cached-reauth-period

```
aaa authentication port-access mac-auth cached-reauth-period <PERIOD>
no aaa authentication port-access mac-auth cached-reauth-period
```

Description

Configures the period during which an authenticated client, which has failed to reauthenticate because the RADIUS server is unreachable, remains authenticated.

The **no** form of the command resets the cached reauthentication period to the default, 3600 seconds.

Parameter	Description
<PERIOD>	Specifies the cached reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring cached reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# cached-reauth-period 300
```

Resetting the cached reauthentication period to the default value:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no cached-reauth-period
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth password

```
aaa authentication port-access mac-auth password {plaintext|ciphertext}<PASSWORD>
no aaa authentication port-access mac-auth password
```

Description

Enables and configures the global password that the switch must use for MAC authentication. The password can be either in ciphertext or plaintext format.

The **no** form of the command disables the password for MAC authentication.

Parameter	Description
{plaintext|ciphertext}<*PASSWORD*>	Specifies the global password to be used by all MAC authenticating devices in either plaintext or ciphertext format.

Examples

Setting the MAC authentication password:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# password plaintext maX99J#
```

Disabling the MAC authentication password:

```
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# no 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
6000 6100	config	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth quiet-period

```
aaa authentication port-access mac-auth quiet-period <PERIOD>
no aaa authentication port-access mac-auth quiet-period
```

Description

Configures the period during which the switch does not try to authenticate a rejected client.

The **no** form of the command resets the quiet period to the default, 60 seconds.

Parameter	Description
<PERIOD>	Specifies the quiet period (in seconds). Default: 60. Range: 0 to 65535.

Examples

Configuring the quiet period on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# quiet-period 65
```

Resetting the quiet period on a port to default:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no quiet-period
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth radius server-group

```
aaa authentication port-access mac-auth radius server-group <GROUP-NAME>
no aaa authentication port-access mac-auth radius server-group <GROUP-NAME>
```

Description

Configures the MAC authentication server group globally or for a particular port.

The **no** form of the command resets the authentication server group to the default value, **radius**.

When configured on a port, the **no** form of the command resets the server group on that port to the globally configured group. If no global RADIUS server group is configured, the **no** form of the command resets the configuration to the default group, **radius**.

When the RADIUS server group for MAC authentication is updated on a port, any existing clients on the port that were authenticated using the previous globally configured group will associate with the new group for the port during the next re-authentication cycle. Any new client that is onboarding on the port after the server group update will associate with the new group immediately.

Parameter	Description
<GROUP-NAME>	Specifies the name of the MAC authentication server group.

Examples

Configuring the RADIUS server group for MAC authentication globally:

```
switch# config
switch(config)# aaa authentication port-access mac-auth
switch(config-macauth)# radius server-group group1
```

Configuring the RADIUS server group for MAC authentication on **1/1/5**:

```
switch(config)# interface 1/1/5
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# radius server-group group2
```

Resetting the RADIUS server group configuration on **1/1/5**:

```
switch(config)# interface 1/1/5
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no radius server-group
```

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 is now configurable on a port
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6000
6100
	`config`
	`config-macauth`
	`config-if-macauth`
		Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth reauth

```
aaa authentication port-access mac-auth reauth
no aaa authentication port-access mac-auth reauth
```

Description

Enables periodic MAC reauthentication of authenticated clients on the port.

The **no** form of the command disables periodic MAC reauthentication on the port.

Examples

Enabling reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# reauth
```

Disabling reauthentication on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no reauth
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access mac-auth reauth-period

```
aaa authentication port-access mac-auth reauth-period <PERIOD>
no aaa authentication port-access mac-auth reauth-period
```

Description

Configures the period after which MAC authenticated clients must be reauthenticated on the port. You must first enable MAC reauthentication on the port before configuring the MAC reauthentication period.

The **no** form of the command resets the MAC reauthentication period to the default, 3600 seconds.

Parameter	Description
<PERIOD>	Specifies the MAC reauthentication period (in seconds). Default: 3600. Range: 1 to 4294967295.

Examples

Configuring the MAC reauthentication period on a port:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# reauth-period 60
```

Resetting the MAC reauthentication period to its default:

```
switch(config-if)# aaa authentication port-access mac-auth
switch(config-if-macauth)# no reauth-period
```

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
6000 6100	config-if	Administrators or local user group members with execution rights for this command.

clear mac-auth statistics

```
clear mac-auth statistics [interface <IF-NAME>]
```

Description

Clears the MAC authentication statistics associated with the port and all the authenticator state machines associated to this port.

If no interface is specified, the statistics is cleared for all MAC authentication enabled ports.

Parameter	Description
<IF-NAME>	Specifies the interface name.

Examples

Clearing MAC authentication statistics on a port:

```
switch# clear mac-auth statistics interface 1/1/1
```

Clearing MAC authentication statistics on all ports:

```
switch# clear mac-auth statistics
```

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
6000 6100	Operator (>) or Manager (#)	Operators 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 port-access mac-auth interface client-status

```
show aaa authentication port-access mac-auth interface {all|<IF-NAME>}
 client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about MAC authentication clients status. The output can be filtered by interface or MAC address.

Parameter	Description
`all`	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing client status information for all ports:

```
switch# show aaa authentication port-access mac-auth interface all client-status

Port Access Client Status Details

Client  AB:CD:DE:FF:AA:BB, 1/1/1
==========================================
  Authentication Details
  ----------------------
    Status                                  : Authenticated
    Type                                    : Pass-Through
    Auth-Method                             : CHAP
    Time Since Last State Change            : 10 secs

  Authentication Statistics
  -------------------------
        Authentication                  : 1
  Authentication Timeout          : 0
  Successful Authentication       : 1
  Failed Authentication           : 0
  Re-Authentication               : 0
  Successful Re-Authentication    : 0
  Failed Re-Authentication        : 0
        Re-Auths When Authenticated     : 0
  Cached Re-Authentication        : 0

Client  DD:CD:AB:CS:EE:OI, 1/1/2
==========================================
  Authentication Details
  ----------------------
    Status                                  : Unauthenticated
    Type                                    : Pass-Through
    Auth-Method                             : CHAP
    Auth Failure reason                     : Server reject/ Server timeout
    Time Since Last State Change            : 15 secs

  Authentication Statistics
  -------------------------
  Authentication                : 1
  Authentication Timeout        : 0
  Successful Authentication     : 0
  Failed Authentication         : 1
```

```
  Re-Authentication             : 0
  Successful Re-Authentication  : 0
  Failed Re-Authentication      : 0
  Re-Auths When Authenticated   : 0
  Cached Re-Authentication      : 0
```

Showing status information for a client:

```
switch# show aaa authentication port-access mac-auth interface 1/1/1 client-status
mac ab:cd:de:ff:aa:bb

Port Access Client Status Details

Client  AB:CD:DE:FF:AA:BB, 1/1/1
========================================
  Authentication Details
  ----------------------
    Status                                : Authenticated
    Type                                  : Pass-Through
    Auth-Method                           : CHAP
    Time Since Last State Change          : 10 secs

  Authentication Statistics
  -------------------------
       Authentication                 : 1
  Authentication Timeout         : 0
  Successful Authentication      : 1
  Failed Authentication          : 0
  Re-Authentication              : 0
  Successful Re-Authentication   : 0
  Failed Re-Authentication       : 0
       Re-Auths When Authenticated    : 0
  Cached Re-Authentication       : 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
6000 6100	Operator (>) or Manager (#)	Operators 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 port-access mac-auth interface port-statistics

`show aaa authentication port-access mac-auth interface {all|<IF-NAME>} port-statistics`

Description

Shows information about MAC authentication ports. The output can be filtered by interface.

Parameter	Description
`all`	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show aaa authentication port-access mac-auth interface all port-statistics

Port 1/1/1
==========

  Client Details
  --------------
    Number of Clients                 : 3
    Number of authenticated clients   : 2
    Number of unauthenticated clients : 1
    Number of authenticating clients  : 0

Port 1/1/2
==========

  Client Details
  --------------
    Number of Clients                 : 4
    Number of authenticated clients   : 2
    Number of unauthenticated clients : 2
    Number of authenticating clients  : 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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 70
Port access policy commands

port-access policy

```
port-access policy <POLICY-NAME>
   [<SEQUENCE-NUMBER>]
   class {ip|ipv6} <CLASS-NAME> action {<REMARK-ACTIONS> | <POLICE-ACTIONS> | <OTHER-
   ACTIONS>}
   comment <text>
```

Description

Creates or modifies a 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 class and one or more policy actions associated with it.

A policy must be applied to a role using the **associate policy** 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 policy name.
<SEQUENCE-NUMBER>	Specifies the policy entry sequence number. Range: 1 to 4294967295.
`class {ip|ipv6} <CLASS-NAME>`	Specifies the class type and name.

<REMARK-ACTIONS>	These remark actions are available:
	`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 keyword or numeric value (0 to 63). See *DSCP keywords and corresponding values* below.

<POLICE-ACTIONS>	These police actions are available:
	`cir kbps <RATE-KBPS>`
	Specifies a Committed Information Rate (CIR) value in kbps. Range: 1 to 4294967295.
	`exceed`
	Specifies the action to take on packets that exceed the rate limit.

<OTHER-ACTIONS>	These other actions are available: `redirect` Selects redirect of all traffic to a captive portal server.
`comment`	Specifies a policy entry comment.

DSCP keywords and corresponding values

Keyword	Value	Description
AF11	10	DSCP 10 (Assured Forwarding Class 1, low drop probability)
AF12	12	DSCP 12 (Assured Forwarding Class 1, medium drop probability)
AF13	14	DSCP 14 (Assured Forwarding Class 1, high drop probability)
AF21	18	DSCP 18 (Assured Forwarding Class 2, low drop probability)
AF22	20	DSCP 20 (Assured Forwarding Class 2, medium drop probability)
AF23	22	DSCP 22 (Assured Forwarding Class 2, high drop probability)
AF31	26	DSCP 26 (Assured Forwarding Class 3, low drop probability)
AF32	28	DSCP 28 (Assured Forwarding Class 3, medium drop probability)
AF33	30	DSCP 30 (Assured Forwarding Class 3, high drop probability)
AF41	34	DSCP 34 (Assured Forwarding Class 4, low drop probability)
AF42	36	DSCP 36 (Assured Forwarding Class 4, medium drop probability)
AF43	38	DSCP 38 (Assured Forwarding Class 4, high drop probability)
CS0	0	DSCP 0 (Class Selector 0: Default)
CS1	8	DSCP 8 (Class Selector 1: Scavenger)
CS2	16	DSCP 16 (Class Selector 2: OAM)
CS3	24	DSCP 24 (Class Selector 3: Signaling)
CS4	32	DSCP 32 (Class Selector 4: Real time)
CS5	40	DSCP 40 (Class Selector 5: Broadcast video)
CS6	48	DSCP 48 (Class Selector 6: Network control)
CS7	56	DSCP 56 (Class Selector 7)
EF	46	DSCP 46 (Expedited Forwarding)

Usage

- An applied policy processes the packet sequentially against policy and class entries in the list, until either the last policy entry in the list has been evaluated or the packet matches an entry. If there is no match, the packet will be dropped by one of the implicit **deny all** IPv4 and IPv6 entries.

- 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. The sequence numbers may be reordered with the **port-access policy <POLICY-NAME> resequence <STARTING-SEQ-NUM> <INCREMENT>** command.
- If a policy is configured without any action, the default action, **permit**, is applied for that policy.

Examples

Creating a policy with several class entries:

```
switch(config)# port-access policy POL1
switch(config-pa-policy)# 10 class ip dns
switch(config-pa-policy)# 20 class ip dhcp
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1

Access Policy Details:
======================

Policy Name   : POL1
Policy Type   : Local
Policy Status :
SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- -----------------------------------
10          dns                          ipv4 permit
20          dhcp                         ipv4 permit
30          test                         ipv4 cir kbps 1024  exceed drop
```

Adding a comment to an existing class entry:

```
switch(config)# port-access policy POL1
switch(config-pa-policy)# 20 comment DHCP-PERMIT
switch(config-pa-policy)# exit
switch(config)# show run port-access policy POL1

port-access policy POL1
    10 class ip dns
    20 class ip dhcp
    20 comment DHCP-PERMIT
    30 class ip test action cir kbps 1024      exceed drop
```

Removing a comment from an existing class entry:

```
switch(config)# port-access policy POL1
switch(config-pa-policy)# no 20 comment
switch(config-pa-policy)# exit
switch(config)# show run port-access policy POL1

port-access policy POL1
    10 class ip dns
    20 class ip dhcp
    30 class ip test action cir kbps 1024  exceed drop
```

Modifying a policy by replacing one class with another at the same sequence number:

```
switch(config)# port-access policy POL1
switch(config-pa-policy)# 10 class ip mds action dscp af21
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1

Access Policy Details:
======================

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ---------------------------------
10          mds                            ipv4 dscp AF21
20          dhcp                           ipv4 permit
30          test                           ipv4 cir kbps 1024  exceed drop
```

Removing a class:

```
switch(config)# port-access policy POL1
switch(config-pa-policy)# no 10
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1

Access Policy Details:
======================

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ---------------------------------
20          dhcp                           ipv4 permit
30          clearpass-web                  ipv4 cir kbps 1024  exceed drop
```

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
6000 6100	`config` The `policy` command takes you into the `config-pa-policy` context where you enter the policy entries.	Administrators or local user group members with execution rights for this command.

port-access policy copy

`port-access policy <POLICY-NAME> copy <DESTINATION-POLICY>`

Description

Copies an existing policy to a new policy.

Parameter	Description
<POLICY-NAME>	Specifies the existing policy name.
<DESTINATION-POLICY>	Specifies the destination policy name.

Examples

Copying a policy:

```
switch(config)# port-access policy POL1 copy POL1_copy
switch(config)# show port-access policy

Access Policy Details:
======================

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ---------------------------------
20          dhcp                         ipv4 permit
30          test                         ipv4 cir kbps 1024 exceed drop

Policy Name   : POL1_copy
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ---------------------------------
20          dhcp                         ipv4 permit
30          test                         ipv4 cir kbps 1024 exceed drop
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

port-access policy resequence

`port-access policy <POLICY-NAME> resequence <STARTING-SEQ-NUM> <INCREMENT>`

Description

Resequences numbering in a policy.

Parameter	Description
<POLICY-NAME>	Specifies the policy to be resequenced.
<STARTING-SEQ-NUM>	Specifies the starting sequence number. Range: 1 to 4294967295.
<INCREMENT>	Specifies the sequence number increment.

Examples

Resequencing a policy starting at 5 with an increment of 10:

```
switch(config)# port-access policy POL1 resequence 5 10
switch(config)# show port-access policy POL1

Access Policy Details:
======================

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
5           dhcp                         ipv4 permit
15          test                         ipv4 cir kbps 1024 exceed drop
```

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
6000 6100	config	Administrators or local user group members with execution rights for this command.

port-access policy reset

`port-access policy <POLICY-NAME> reset`

Description

Resets the policy configuration to match the current hardware configuration of the policy.

Parameter	Description
<POLICY-NAME>	Specifies the name of the policy to be reset.

Examples

Resetting a policy:

```
switch(config)# port-access policy POL2
switch(config-pa-policy)# 20 class ip dhcp
switch(config-pa-policy)# 40 class test2 action cir kbps 1024 exceed drop
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL1-V2

Access Policy Details:
======================

Policy Name   : POL2
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                         TYPE ACTION
----------- ----------------------------- ---- ---------------------------------
20          dhcp                          ipv4 permit
40          test2                         ipv4 cir kbps 1024 exceed drop

switch(config)# port-access policy POLV2
switch(config-pa-policy)# 50 class ip test3 action cir kbps 1024 exceed drop
switch(config-pa-policy)# no 20
switch(config-pa-policy)# exit
switch(config)# show port-access policy POL2

Access Policy Details:
======================

Policy Name   : POL2
Policy Type   : Local
Policy Status : Rejected

SEQUENCE    CLASS                         TYPE ACTION
----------- ----------------------------- ---- ---------------------------------
40          test2                         ipv4 cir kbps 1024 exceed drop
50          test3                         ipv4 cir kbps 1024 exceed drop

switch(config)# port-access policy POK2 reset
Following policy entries will be removed:
class ip test3 action cir kbps 1024 exceed drop

Following policy entries will be added:
20 class ip dhcp

Do you want to continue (y/n)? y
switch(config)# show port-access policy POL2

Access Policy Details:
======================
```

```
Policy Name   : POL1-V2
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ---------------------------------
20          dhcp                           ipv4 permit
40          test2                          ipv4 cir kbps 1024 exceed drop
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

clear port-access policy hitcounts

`clear port-access policy <POLICY-NAME> hitcounts {port|client}`

Description

Clears statistics and conform rate of a policy applied on a port or client.

Parameter	Description
<POLICY-NAME>	Specifies the policy name.
`port`	Selects port mode.
`client`	Selects client mode.

Examples

Clearing policy hit counts:

```
switch# show port-access policy POL6 hitcounts port

Port Access Policy Hit-Counts Details:
======================================

Policy Name   : POL4
Policy Type   : Local
```

```
Policy Status : Applied

SEQUENCE CLASS             TYPE ACTION                              CUR-RATE(kbps)
-------- ----------------- ---- ----------------------------------- --------------
3        test8             ipv4 cir kbps 1024 exceed drop           512

Class Name : dhcp
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                               HIT-COUNT
----------- --------------------------------------------------------- -----------
10          match icmp any any count                                  0

Class Name : clearpass-web
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                               HIT-COUNT
----------- --------------------------------------------------------- -----------
15          match udp any any count                                   15101830

Class Name : web-traffic
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                               HIT-COUNT
----------- --------------------------------------------------------- -----------
10          match any any any count                                   241
20          match any 10.1.1.1 10.1.1.2 dscp AF11 count               50

Class Name : class6
Class Type : ipv6

SEQUENCE    CLASS-ENTRY                                               HIT-COUNT
----------- --------------------------------------------------------- -----------
10          match any any any count                                   173
20          match icmpv6 2001:db8:a::123 2001:db8:a::125 dscp AF11
             count                                                    32
switch#
switch# clear port-access policy POL6 hitcounts port
switch#
switch# show port-access policy POL6 hitcounts port

Port Access Policy Hit-Counts Details:
======================================

Policy Name   : POL4
Policy Type   : Local
Policy Status : Applied

SEQUENCE CLASS             TYPE ACTION                              CUR-RATE(kbps)
-------- ----------------- ---- ----------------------------------- --------------
3        test8             ipv4 cir kbps 1024 exceed drop           512

Class Name : dhcp
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                               HIT-COUNT
----------- --------------------------------------------------------- -----------
10          match icmp any any count                                  0

Class Name : clearpass-web
Class Type : ipv4
```

```
SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
15          match udp any any count                                    0

Class Name : web-traffic
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match any any any count                                    0
20          match any 10.1.1.1 10.1.1.2 dscp AF11 count                0

Class Name : class6
Class Type : ipv6

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match any any any count                                    0
20          match icmpv6 2001:db8:a::123 2001:db8:a::125 dscp AF11
             count                                                     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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access policy

`show port-access policy [<POLICY-NAME>]`

Description

Shows various aspects of policies and their current usage. Details of a policy including the content of a specific policy is shown.

Policy type values:

- **Local**—User configured policy
- **Downloaded**—Downloaded user policy
- **RADIUS**—Policy obtained from the RADIUS server

Policy status values:

- **Applied**—Policy is successfully applied in the hardware.
- **Rejected**—Policy is not supported in the hardware.
- **In-Progress**—Policy is being processed in the hardware.
- **Failed**—Displayed when the switch fails to apply the policy configuration because the TCAM resources are unavailable or full.

Base Policy Values:

- **Name of the policy**—Policy associated with the RADIUS overridden base role.
- **N/A**—Non-RADIUS policy or policy derived from RADIUS attributes such as Filter ID or [Aruba-]NAS-Filter-Rule

ACL Names Values:

- **Name of the ACL**—Name of the ACL associated with the RADIUS policy derived from RADIUS Filter-ID attribute.
- **N/A**—Non-RADIUS policy or policy derived from [Aruba-]NAS-Filter-Rule RADIUS attribute.

If a policy is configured without any action, the **show** command will represent such an entry with the **permit** action .

Parameter	Description
<POLICY-NAME>	Specifies the policy name.

Examples

Showing information for all policies:

```
switch(config)# show port-access policy

Access Policy Details:
======================

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied
Base Policy:  N/A
ACL Name:  N/A

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
20          dhcp                         ipv4 permit
30          test                         ipv4 cir kbps 1024 exceed drop

Policy Name   : POL1_copy
Policy Type   : Local
Policy Status : Applied
Base Policy: N/A
ACL Name:  N/A

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
20          dhcp                         ipv4 permit
30          test                         ipv4 cir kbps 1024 exceed drop
```

Showing information for a particular policy:

```
switch(config)# show port-access policy RADIUS_115315236
Access Policy Details:
----------------------

Policy Name   : RADIUS_115315236
Policy Type   : Radius
Policy Status : Applied
Base Policy   : N/A
ACL Names     : DHCP, WebServices-Student

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------
10          RADIUS_3241199543_2521983626 ipv4 permit


switch(config)# show port-access policy RADIUS_407949976
Access Policy Details:
----------------------

Policy Name   : RADIUS_407949976
Policy Type   : Radius
Policy Status : Applied
Base Policy   : test_policy_test_cppm_role-3006-1
ACL Names     : N/A


SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------
10          RADIUS_407949976_4016176641  ipv4 permit
```

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 output modified to display **Base Policy** and **ACL Names**.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access policy hitcounts

`show port-access policy <POLICY-NAME> hitcounts {port | client}`

Description

Shows port access hit count statistics.

Parameter	Description
<POLICY-NAME>	Specifies the policy name.
`port`	Selects port mode.
`client`	Selects client mode.

Examples

Showing policy hit counts (statistics) with current rate:

```
switch# show port-access policy POL6 hitcounts port

Port Access Policy Hit-Counts Details:
======================================

Policy Name   : POL1
Policy Type   : Local
Policy Status : Applied

SEQUENCE CLASS       TYPE ACTION                                CUR-RATE(kbps)
-------- ----------- ---- ------------------------------------  --------------
30       test8       ipv4 cir kbps 1024 exceed  drop         512

Class Name : dhcp
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match icmp any any count                                   982150

Class Name : clearpass-web
Class Type : ipv4

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
70          match udp any any count                                    15101830


Class Name : class6
Class Type : ipv6

SEQUENCE    CLASS-ENTRY                                                HIT-COUNT
----------- ---------------------------------------------------------- -----------
10          match any any any count                                    0
20          match icmpv6 2001:db8:a::123 2001:db8:a::125 dscp AF11
             count                                                     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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

associate policy

```
associate policy <POLICY-NAME>
no associate policy <POLICY-NAME>
```

Description

Associates the policy with the current role.

The **no** form of this command dissociates the policy from the role.

Parameter	Description
<POLICY-NAME>	Specifies the policy name to associate with the current role. Range: Up to 64 characters. **NOTE:** Only those policies created by using the **port-access policy** command are allowed to be associated with a role. Policies created using the **policy** command are not allowed to be associated with a role. Policies that are of the downloaded type are not allowed to be associated with a role.

Examples

Associating a policy with a role:

```
switch(config)# port-access role role01
switch(config-pa-role)# associate policy policy01
```

Dissociating a policy from the role:

```
switch(config-pa-role)# no associate policy poilcy01
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

auth-mode

```
auth-mode {client-mode | device-mode | multi-domain}
```

Description

Configures the authentication mode for the clients that are associated with the current role.

Parameter	Description
`client-mode`	Selects client mode. In this mode, all clients connecting to the port are sent for authentication.
`device-mode`	Selects device mode. In this mode, only the first client connecting to the port is sent for authentication. Once this client is authenticated, the port is considered as open and all subsequent clients trying to connect on that port are not sent for authentication.
`multi-domain`	Selects multidomain mode. In this mode only one voice device is allowed to be authenticated in addition to the configured data devices on a port. By default only one data device is allowed to be authenticated on the multidomain mode along with one voice device. You can configure the maximum number of data devices allowed with the **aaa authentication port-access client-limit multi-domain** command. If a second voice device or a data device greater than the configured data client limit onboards, a violation is triggered. You must configure a voice VLAN for IP phones to onboard a voice device in the multidomain authentication mode. To authorize a voice device, you must perform one of the following: ▪ Configure the AAA server to send the **Aruba-Device-Traffic-Class** Aruba VSA with value **1**. ▪ Configure the **device-traffic-class** parameter in the role to be applied to indicate a voice device. Without this VSA value or the device type in the role, the switch considers the voice device as a data device.

Examples

Configuring the client authentication mode:

```
switch(config-pa-role)# auth-mode client-mode
```

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

Command History

Release	Modification
10.08	Added **multi-domain** parameter
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

cached-reauth-period

```
cached-reauth-period [<PERIOD>]
no cached-reauth-period
```

Description

Enables cached reauthentication, setting the period after which clients that associated with the current role must be reauthenticated.

The **no** form of this command disables cached authentication.

Parameter	Description
<PERIOD>	Specifies the cached reauthentication period (in seconds) for clients associated with the role. Default: 30. Range: 30 to 4294967295.

Examples

Enabling cached reauthentication and setting its period to 200 seconds:

```
switch(config-pa-role)# cached-reauth-period 200
```

Disabling cached reauthentication:

```
switch(config-pa-role)# no cached-reauth-period
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

client-inactivity timeout

```
client-inactivity timeout {<CLIENT-INACTIVITY-PERIOD> | none}
no client-inactivity timeout
```

Description

Configures the period that the switch waits for a response from a client after which it removes the client from the role.

The **no** form of the command resets the timeout period to the default.

Parameter	Description
<CLIENT-INACTIVITY-PERIOD>	Specifies the client inactivity time (in seconds). Default: Dynamic client age-out. Range: 60 to 4294967295
`none`	Selects no client deletion due to inactivity.

Examples

Configuring client inactivity timer for a role:

```
switch(config-pa-role)# client-inactivity timeout 3600
```

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

Command History

Release	Modification
10.14	The range of the command has been modified from 60 to 4294967295 seconds.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000	`config-pa-role`	Administrators or local user group members with execution rights

Platforms	Command context	Authority
6100	The `port-access role` command takes you into the `config-pa-role` context.	for this command.

description

`description <ROLE-DESCRIPTION>`

Description

Configures the role description.

Parameter	Description
<ROLE-DESCRIPTION>	Specifies the role description. Range: Up to 255 characters.

Examples

Configuring the role description:

```
switch(config-pa-role)# description student role
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

device-traffic-class

```
device-traffic-class voice
no device-traffic-class [voice]
```

Description

Configures the voice class of client to associate with the role.

This attribute is applicable only to **critical-voice-role** role. It is not applicable to other special roles such as, **preauth-role**, **reject-role**, and **fallback-role**.

The **no** form of the command resets the class of client to the default, data.

Usage

Traffic class of a client will not be considered as voice unless **device-traffic-class** is set to **voice** the role. In the multidomain mode, clients with a role that do not have the value of the **device-traffic-class** attribute set to voice will be considered as data device.

Examples

Configuring voice device traffic class for role **role01**:

```
switch(config)# port-access role role01
switch(config-pa-role)# device-traffic-class voice
```

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

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config-pa-role` The **port-access role** command takes you into the **config-pa-role** context.	Administrators or local user group members with execution rights for this command.

mtu

`mtu <MTU-SIZE>`

Description

Configures the MTU (maximum transmission unit) size of a client for a role.

Parameter	Description
<MTU-SIZE>	Specifies the MTU size in bytes. Range: 68 to 9198.

Examples

Configuring client MTU size:

```
switch(config-pa-role)# mtu 9198
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

poe-allocate-by

```
poe-allocate-by {class | usage}
no poe-allocate-by {class | usage}
```

Description

Configures the PoE allocation method for the configured port-access role. If the allocation method is not configured, the power allocation method configured on the interface is used.

The **no** form of this command removes the configuration.

Downloadable user role (DUR) is not supported on 6000 and 6100 Switch Series.

Parameter	Description
`class`	Configures the PoE class-based allocation method.
`usage`	Configures the PoE usage-based allocation method.

Examples

Configuring **class** as PoE allocation method for the role **role01**:

```
switch(config)# port-access role role01
switch(config-pa-role)# poe-allocate-by class
```

Removing PoE allocation method configured for the port-access role:

```
switch(config)# port-access role role01
switch(config-pa-role)# no poe-allocate-by
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

poe-priority

```
poe-priority {critical | high | low}
no poe-priority
```

Description

Configures the power distribution priority for the port access roles. High power consumption can be prevented using the **poe-priority** control mechanism.

The **no** form of this command restores the power distribution to its default priority.

Parameter	Description
`critical`	Selects critical priority.
`high`	Selects high priority.
`low`	Selects low priority.

Examples

Configuring PoE priority for a new role:

```
switch(config)# port-access role role01
switch(config-pa-role)# poe-priority critical
```

Resetting PoE priority for the role to its default:

```
switch(config)# port-access role role01
switch(config-pa-role)# no poe-priority
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

port-access role

```
port-access role <ROLE-NAME>
no port-access role <ROLE-NAME>
```

Description

Creates a new port access role or modifies an existing role. This command takes you into the **config-pa-role** context. A maximum of 32 port access roles can be created.

The **no** form of this command deletes a role.

Parameter	Description
<ROLE-NAME>	Specifies the role name. Range: Up to 64 characters.

Examples

Creating a new role:

```
switch(config)# port-access role basic01
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

reauth-period

```
reauth-period <PERIOD>
no reauth-period
```

Description

Configures the period after which clients that associated with the current role must be reauthenticated.

The reauthentication period configured here takes precedence over the reauthentication period configured at the port level.

Parameter	Description
<PERIOD>	Specifies the reauthentication period (in seconds) for clients associated with the role. Default: None. Range: 1 to 4294967295. A reauthentication period of less than 60 seconds is not recommended.

Examples

Configuring reauthentication period:

```
switch(config-pa-role)# reauth-period 3000
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

session timeout

```
session-timeout <SESSION-TIMEOUT>
no session-timeout
```

Description

Configures the session timeout for the role. After the timeout period, the session is disconnected.

Parameter	Description
<SESSION-TIMEOUT>	Specifies the session timeout (in seconds). Range: 1 to 4294967295. A timeout of less than 60 seconds is not recommended.

Examples

Configuring session timeout for a role:

```
switch(config-pa-role)# session timeout 3600
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

show aaa authentication port-access interface client-status

```
show aaa authentication port-access interface {all | <IF-NAME>}
client-status [mac <MAC-ADDRESS>]
```

Description

Shows information about the status of the role applied on ports.

Parameter	Description
`all`	Specifies all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing information about a client:

```
switch# show aaa authentication port-access interface all client-status mac
00:00:00:00:00:01

Port Access Client Status Details

Client 00:00:00:00:00:01
============================
  Session Details
  ---------------
    Port         : 1/7/24
    Session Time : 151s

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : mac-auth - Authenticated, dot1x - Not attempted

  Authorization Details
  ---------------------
    Role   : UserRole_1
    Status : Applied
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access role

```
show port-access role {local | radius | name <ROLE-NAME>}
```

Roles downloaded from ClearPass Policy Manager are available on the 4100i Switch Series. They are not available on the 6000 and 6100 Switch Series.

Description

Shows information about roles configured locally, or downloaded from the RADIUS server.

Displays information only about the attributes defined for the role. The base policy name will be suffixed with * for RADIUS overridden roles.

Parameter	Description
`local`	Shows information about locally configured roles.
`radius`	Shows information about roles downloaded from the RADIUS server.
<ROLE-NAME>	Specifies the role name.

Examples

Showing locally configured role information:

```
switch# show port-access role local
Role Information:
Name  : local_role_01
Type  : local
-----------------------------------------------
Reauthentication Period             : 333 secs
Cached Reauthentication Period      : 300 secs
Access VLAN Name                    : Hpe
VLAN Group Name                     : group1
PoE Priority                        : low
Policy                              : deny-http-policy
Private-VLAN Port-Type              : secondar
```

Showing locally configured role information:

```
switch# show port-access role local

Role Information:

   Name  : local_role_01
   Type  : local
   -----------------------------------------------
     Reauthentication Period             : 333 secs
     Cached Reauthentication Period      : 300 secs
     Access VLAN Name                    : Hpe
     VLAN Group Name                     : group1
     PoE Priority                        : low
     Policy                              : deny-http-policy
     Private-VLAN Port-Type              : secondary
```

Showing information for roles downloaded from a RADIUS server:

```
switch# show port-access role radius
Role Information:
Attributes overridden by RADIUS are prefixed by '*'.

Name : RADIUS_21963402
Type : radius
-----------------------------------------------
Reauthentication Period: 333 secs
Access VLAN: 10
VLAN Group Name: group1
STP Administrative Edge Port : true
PoE Priority : low
PoE Allocation Method: class
Captive Portal Profile : testcpprof_29451201
Policy : PERMIT-ALL_87364653
Private-VLAN Port-Type : secondary
```

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

Command History

Release	Modification
10.12	The following changes were introduced: ■ Command output updated to display information only about the attributes defined for the role. ■ Updated output to display **PoE Allocation method**. ■ The base policy name will be suffixed with * for RADIUS overridden roles.
10.09.1000	Added captive portal support to the 4100i, 6000, 6100 Switch Series
10.08	Updated RADIUS role example with radius-overridden attributes
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

stp-admin-edge-port

```
stp-admin-edge-port
no stp-admin-edge-port
```

Description

Configures the port as a spanning tree administrative edge port for the role. This configuration removes the port participation from STP interactions when onboarding devices. This in turn helps in faster onboarding of devices.

The **no** form of the command disables STP edge port functionality.

If the port receives STP BPDU on the STP administrative edge configured port, the port will move to the STP state. You must configure the port as an STP administrative edge port only if you are sure that the connected device will not participate in STP interactions.

Example

Configuring STP edge port for a role:

```
switch(config)# port-access role role01
switch(config-pa-role)# stp-admin-edge-port
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

trust-mode

```
trust-mode [dscp | cos | none]
no trust-mode
```

Description

Configures QoS trust mode for the role.

The **no** form of this command configures the default trust mode for the role.

Parameter	Description
`dscp`	Selects trust DSCP and retain 802.1p priority.

Parameter	Description
`cos`	Selects trust 802.1p and retain DSCP or IP-ToS.
`none`	Selects no trusting of priority fields.

Examples

Configuring DSCP trust mode for a role:

```
switch(config)# port-access role role01
switch(config-pa-role)# trust-mode dscp
```

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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

vlan

```
vlan {access | trunk native | trunk allowed} <VLAN-ID>
no vlan {access | trunk native | trunk allowed} <VLAN-ID>

vlan {access name | trunk native name | trunk allowed name} <VLAN-NAME>
no vlan {access name | trunk native name | trunk allowed name} [<VLAN-NAME>]
```

Description

Configures VLAN IDs or VLAN names, and VLAN modes for a port access role. You can configure either VLAN IDs or VLAN names, or a combination of both for a role.

The **no** form of the command deletes the VLAN configuration from the role. For trunk allowed VLAN names, you can delete the VLAN names individually or all names at once.

Parameter	Description
`access <VLAN-ID>`	Specifies the VLAN ID for the access VLAN. Supports a single VLAN ID in the range 1 to 4094.

Parameter	Description
`trunk native <VLAN-ID>`	Specifies the native VLAN ID on the trunk interface. Supports a single VLAN ID. Range: 1 to 4094.
`trunk allowed <VLAN-ID>`	Specifies the list of tagged or allowed VLANs on the trunk interface. Supports a list of VLAN IDs. Range: 1 to 4094.
`access name <VLAN-NAME>`	Specifies the VLAN name for the access VLAN. Supports a single VLAN name. Range: Up to 32 characters.
`trunk native name <VLAN-NAME>`	Specifies the native VLAN name on the trunk interface. Supports a single VLAN name. Range: Up to 32 characters
`trunk allowed name <VLAN-NAME>`	Specifies the tagged or allowed VLAN name on the trunk interface. Supports a single VLAN name. Range: Up to 32 characters. The switch supports a maximum of 50 trunk allowed VLAN names.

Usage

Note the following points when configuring the VLAN IDs and names for a role:

- For VLAN access and VLAN trunk native respectively, it is recommended to configure only one of either VLAN ID or name for a role. In case both VLAN ID and name are configured, then VLAN ID takes precedence and is applied with the role.

Platform	Maximum VLAN IDs per role	Maximum VLAN Namesper role	Total VLANs (ID + Name) per role
6000	50	50	50
6100	50	50	50

Examples

Configuring VLAN modes and VLAN IDs for a new role:

```
switch(config)# port-access role role01
switch(config-pa-role)# vlan trunk native 10
switch(config-pa-role)# vlan trunk allowed 11-15
switch(config-pa-role)# vlan access 50
```

Configuring VLAN modes and VLAN names for a new role:

```
switch(config)# port-access role role10
switch(config-pa-role)# vlan trunk native name hpe01
switch(config-pa-role)# vlan trunk allowed name data
switch(config-pa-role)# vlan trunk allowed name voice
switch(config-pa-role)# vlan trunk allowed name video
```

Deleting VLAN configuration from a role:

```
switch(config-pa-role)# no vlan trunk native 10
switch(config-pa-role)# no vlan trunk allowed 10-15
switch(config-pa-role)# no vlan access 50
```

Deleting trunk allowed VLAN names from a role individually:

```
switch(config-pa-role)# no vlan trunk native name hpe01
switch(config-pa-role)# no vlan trunk allowed name data
switch(config-pa-role)# no vlan trunk allowed name voice
switch(config-pa-role)# no vlan trunk allowed name video
```

Deleting trunk allowed VLAN names from a role all at once:

```
switch(config-pa-role)# no vlan trunk native name hpe01
switch(config-pa-role)# no vlan trunk allowed 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
6000 6100	`config-pa-role` The `port-access role` command takes you into the `config-pa-role` context.	Administrators or local user group members with execution rights for this command.

port-access security violation action

```
port-access security violation action {notify | shutdown}
no port-access security violation action
```

Description

Configures the action that the switch must take whenever a security violation occurs at a port, such as the number of clients exceeding the configured client limit. This command can be issued from the interface (**config-if**) or Link Aggregation Group (**config-lag-if**) contexts.

The **no** form of the command resets the action to the default action, notify.

Parameter	Description
`notify`	Specifies that the switch notifies any security violation as an event or log in the syslog server, and also sends an SNMP trap notification. This action is the default. The format of the event log that is generated for notifying the security violation is: `Client limit exceeded on port` **`<PORT>`**`, caused by an unauthenticated client` **`<MAC-ADDRESS>`**.
`shutdown`	Specifies that the switch shuts down the port where the client limit has exceeded. A port that is shut down can be configured to auto-recover after a recovery period that can be configured with the **port-access security violation action shutdown auto-recovery** and **port-access security violation action shutdown recovery-timer** commands.

Examples

Configuring the shutdown security violation action for interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access security violation action shutdown
```

Resetting the security violation action to the default value:

```
switch(config-if)# no port-access security violation action
```

Configuring the shutdown security violation action for a LAG port:

```
switch(config)# interface lag 1
switch(config-lag-if)# port-access security violation action shutdown
```

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

Command History

Release	Modification
10.13	This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

port-access security violation action shutdown auto-recovery

```
port-access security violation action shutdown auto-recovery {enable | disable}
no port-access security violation action shutdown auto-recovery {enable | disable}
```

Description

Configures auto-recovery of the port when the security violation action is configured as shutdown.

This configuration allows the port, that is shut down when a security violation occurs, to be automatically enabled after the recovery timer expires.

The **no** form of the command resets auto-recovery to the default, disable.

Parameter	Description
`enable`	Enables auto-recovery of port when the security violation action is configured as shutdown.
`disable`	Disables auto-recovery of port when the security violation action is configured as shutdown.

Examples

Enabling auto-recovery of port:

```
switch(config-if)# port-access security violation action shutdown auto-recovery
enable
```

Disabling auto-recovery of port:

```
switch(config-if)# no port-access security violation action shutdown auto-recovery
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

port-access security violation action shutdown recovery-timer

```
port-access security violation action shutdown recovery-timer <RECOVERY-TIME>
no port-access security violation action shutdown recovery-timer
```

Description

Configures security violation recovery timer for the port when the security violation action is configured as shutdown.

The **no** form of the command resets the shutdown recovery timer to the default, 10.

Parameter	Description
<RECOVERY-TIME>	Specifies the recovery timer (in seconds) after which the port, which is shut down because of security violation, is automatically enabled. Default: 10. Range: 10 to 600.

Examples

Configuring the shutdown recovery-timer on a port:

```
switch(config-if)# port-access security violation action shutdown recovery-timer
60
```

Resetting the shutdown recovery-timer to the default value:

```
switch(config-if)# no port-access security violation action shutdown recovery-
timer
```

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
6000 6100	`config-if`	Administrators or local user group members with execution rights for this command.

show interface

`show interface <INTERFACE-NAME>`

Description

Displays active configurations and operational status information for interfaces including the reason for the port shutdown because of a security violation at the port.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface name.

Examples

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 port-access aaa violation interface

`show port-access aaa violation interface {all|<INTERFACE>}`

Description

Shows information about violations that have occurred and the count of violations for port access authentication methods at the interfaces.

Parameter	Description
`all`	Specifies all interfaces.
<INTERFACE>	Specifies the interface name or a comma-separated list of interfaces, or a hyphen-separated interface range.

Examples

Showing information for violations for all interfaces:

```
switch# show port-access aaa violation interface all

Client limit exceeded violation status

-----------------------------------------------------
   Port      Violation      Violation-Count
-----------------------------------------------------
   1/1/1       No                0
   1/1/2       Yes               10
   1/1/5       No                10
```

Showing information for violations on interfaces 1/1/1 to 1/1/2:

```
switch# show port-access aaa violation interface 1/1/1-1/1/2

Client limit exceeded violation status

-----------------------------------------------------
   Port      Violation      Violation-Count
-----------------------------------------------------
   1/1/1       No                0
   1/1/2       Yes               10
```

Showing information when no violation action is configured:

```
switch# show port-access aaa violation interface 1/1/1

Port-access aaa violation is not configured
```

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

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access port-security violation client-limit-exceeded interface

```
show port-access port-security violation client-limit-exceeded interface
{all|<INTERFACE>}
```

Description

Shows information on the number of client-limit-exceeded security violations that have occurred. The output can be filtered by interface.

Parameter	Description
`all`	Specifies all interfaces.
<INTERFACE>	Specifies the interface name or a comma-separated list of interfaces, or a hyphen-separated interface range.

Examples

Showing information for all ports:

```
switch# show port-access port-security violation client-limit-exceeded interface
all

Client limit exceeded violation status

-----------------------------------------------------
   Port      Violation      Violation-Count
-----------------------------------------------------
   1/1/1       No                 0
   1/1/2       Yes                10
   1/1/5       No                 10
```

Showing information for a port range:

```
switch# show port-access port-security violation client-limit-exceeded interface
1/1/1-1/1/2

Client limit exceeded violation status

-----------------------------------------------------
   Port      Violation      Violation-Count
-----------------------------------------------------
   1/1/1       No                 0
   1/1/2       Yes                10
```

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

Command History

Release	Modification
10.08	Syntax modified from **show port-access security violation client-limit-exceeded interface {all|<INTERFACE-NAME>}** to **show port-access port-security violation client-limit-exceeded interface {all|<INTERFACE-NAME>}**
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

associate-vlan

```
associate-vlan <VLAN-ID>
no associate-vlan <VLAN-ID>
```

Description

Associates VLANs with an existing VLAN group.

The **no** form of this command removes the association of the VLAN with the specified VLAN group.

Parameter	Description
<VLAN-ID>	Specifies the VLAN or a specific set of VLANs. Range 1 to 4094.

Examples

Associating VLANs with **group1**:

```
switch(config)# port-access vlan-group group1
switch(config-pa-vlan-group)# associate-vlan 5,10-15,20,21
```

Associating additional VLANs with **group1**:

```
switch(config)# port-access vlan-group group1
switch(config-pa-vlan-group)# associate-vlan 30-40
```

Dissociating VLANs 10-15 from VLAN **group1**:

```
switch(config-pa-vlan-group)# no associate-vlan 10-15
```

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
6000 6100	`config-pa-vlan-group`	Administrators or local user group members with execution rights for this command.

port-access vlan-group

```
port-access vlan-group <NAME>
no port-access vlan-group <NAME>
```

Description

Creates the specified VLAN group (if it does not already exist) and then enters its context **config-pa-vlan-group**. For an existing VLAN group, this command enters the context of the specified VLAN group.

The **no** form of this command removes the specified VLAN group.

In order for the group to be applied to a client, VLANs associated to the group should be configured on the switch. If not, the role displays an error.

Parameter	Description
<NAME>	Specifies the name of the VLAN group. Range 2 to 32 characters.

Examples

Creating VLAN **group1** and associating VLANs with it:

```
switch(config)# port-access vlan-group group1
switch(config-pa-vlan-group)# associate-vlan 5,10-15,20,21
```

Dissociating VLANs 10-15 from VLAN **group1**:

```
switch(config-pa-vlan-group)# no associate-vlan 10-15
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

show running-config port-access vlan-group

```
show running-config port-access vlan-group
```

Description

Shows information for all configured VLAN groups.

Example

Showing the port access VLAN group configuration:

```
switch# show running-config port-access vlan-group
...
port-access vlan-group group1
    associate-vlan 5,20,21,30-40
port-access vlan-group group2
    associate-vlan 50-60,75-85
...
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

portfilter

```
portfilter <INTERFACE-LIST>
no portfilter [<INTERFACE-LIST>]
```

Description

Configures the specified ports so they do not egress any packets that were received on the source port specified in interface context.

The **no** form of this command removes the port filter setting from one or more ingress ports/LAGs.

This configuration will disable flow tracking statistics collection.

Parameter	Description
<INTERFACE-LIST>	Specifies a list of ports/LAGs to be blocked for egressing. Specify a single interface or LAG, or a range as a comma-separated list, or both. For example: `1/1/1`, `1/1/3-1/1/6`,`lag2`, `lag1-lag4`.

Usage

When a port filter configuration is applied on the same ingress physical port/LAG, the configuration is updated with the new sets of egress ports/LAGs that are to be blocked for egressing and that are not a part of its previous configuration. Duplicate updates on an existing port filter configuration are ignored.

When egress ports/LAGs are removed from the existing port filter configuration of an ingress port/LAG, egressing is allowed again on those egress ports/LAGs for all packets originating from the ingress port/LAG.

The **no portfilter [*<IF-NAME-LIST>*]** command removes port filter configurations from the egress ports/LAGs listed in the *<IF-NAME-LIST>* parameter only. All other egress ports/LAGs in the port filter configuration of the ingress port/LAG remain intact.

If no physical ports or LAGs are provided for the **no portfilter** command, the command removes the entire port filter configuration for the ingress port/LAG.

Examples

Creating a filter that prevents packets received on port **1/1/1** from forwarding to ports **1/1/3-1/1/6** and to LAGs **1** through **4**:

```
switch(config)# interface 1/1/1
switch(config-if)# portfilter 1/1/3-1/1/6,lag1-lag4
```

Creating a filter that prevents packets received on LAG **1** from forwarding to ports **1/1/6** and LAGs **2** and **4**:

```
switch(config)# interface lag 1
switch(config-lag-if)# portfilter 1/1/6,lag2,lag4
```

Removing filters from an existing configuration that allows back packets received on port **1/1/1** to forward to ports **1/1/6** and LAGs **3** and **4**:

```
switch(config)# interface 1/1/1
switch(config-if)# no portfilter 1/1/6,lag3,lag4
```

Removing all filters from an existing configuration that allows back packets received on LAG **1** to forward to all the ports and LAGs:

```
switch(config)# interface lag 1
switch(config-lag-if)# no portfilter
```

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

Command History

Release	Modification
10.14	Added information related to role based IPFIX.
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.

show portfilter

`show portfilter [<IFNAME>]`

Description

Displays filter settings for all interfaces or a specific interface.

Parameter	Description
<IFNAME>	Specifies the ingress interface name. Specifies one of these values:

Parameter	Description
	▪ *<FQDN>*: a fully qualified domain name. ▪ *<IPV4>*: an IPv4 address. ▪ *<IPV6>*: an IPv6 address.

Examples

Displaying all port filter settings on the switch:

```
switch# show portfilter
Incoming   Blocked
Interface  Outgoing Interfaces
-------------------------------------------------------------------------------
1/1/1      1/1/3-1/1/6,lag1-lag2
1/1/3      1/1/1,1/1/5,1/1/7,1/1/9,1/1/11,1/1/13,1/1/15,1/1/17,1/1/19,1/1/21,
           1/1/23,1/1/25,1/1/27,1/1/29,1/1/31,1/1/33,1/1/35
lag2       1/1/1,1/1/3-1/1/6
```

Displaying the port filter settings for port **1/1/1**:

```
switch# show portfilter 1/1/1
Incoming   Blocked
Interface  Outgoing Interfaces
-------------------------------------------------------------------------------
1/1/1      1/1/3-1/1/6,lag1-lag2
```

Displaying the port filter settings for **LAG2**:

```
switch# show portfilter lag2
Incoming   Blocked
Interface  Outgoing Interfaces
-------------------------------------------------------------------------------
lag2       1/1/1,1/1/3-1/1/6
```

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.

port-access port-security

```
port-access port-security {enable | disable}
no port-access port-security {enable | disable}
```

Description

Enables or disables port security globally or at the port level.

Examples

Enabling port security globally:

```
switch(config)# port-access port-security enable
```

Disabling port security globally:

```
switch(config)# port-access port-security disable
```

Enabling port security on a port:

```
switch(config-if)# port-access port-security enable
```

Disabling port security on a port:

```
switch(config-if)# port-access port-security disable
```

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
6000 6100	`config` `config-if`	Administrators or local user group members with execution rights for this command.

port-access port-security client-limit

```
port-access port-security client-limit <CLIENTS>
no port-access port-security client-limit
```

Description

Configures the maximum number of clients that are allowed on a port. After configuring the maximum clients limit, the MAC addresses of the clients can be learned by one of the following methods:

- User can manually configure all MAC addresses by using the **mac-address** command.
- User can allow the port to dynamically learn all MAC addresses.
- User can configure a fixed number of MAC addresses and allow the switch to learn the remaining addresses dynamically.

The **no** form of the command resets the number of clients to the default, 1.

Parameter	Description
<CLIENTS>	Specifies the maximum number of clients. Default: 1. Range: **0 to 32 (4100i, 6000, 6100). 0 to 64 (8325, 10000). 0 to 32 (6200). 0 to 64 (6300, 6400).** **NOTE:** If client limit is configured to 0, the port will not learn any MAC address from inbound traffic and will be blocked indefinitely. An administrator can use this along with the port-access security violation configuration to get notified of a client attempting to connect to a port.

Examples

Configuring client limit on a port:

```
switch(config-if)# port-access port-security enable
switch(config-if-port-security)# client-limit 24
```

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
6000 6100	config-if-port-security	Administrators or local user group members with execution rights for this command.

port-access port-security mac-address

```
port-access port-security mac-address <MAC-ADDRESS>
no port-access port-security mac-address <MAC-ADDRESS>
```

Description

Configures a static client (current interface (port) context) MAC address.

The **no** form of this command removes an authorized static client from the port.

Parameter	Description
<MAC-ADDRESS>	Specifies the static client MAC address.

Examples

Configuring a static client on a port:

```
switch(config-if)# port-access port-security
switch(config-if-port-security)# mac-address aa:bb:cc:dd:ee:ff
```

Deleting a static client on a port:

```
switch(config-if)# port-access port-security
switch(config-if-port-security)# no mac-address aa:bb:cc:dd:ee:ff
```

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
6000 6100	`config-if-port-security`	Administrators or local user group members with execution rights for this command.

show port-access port-security interface client-status

```
show port-access port-security interface {all|<IF-NAME>}
     client-status [mac <MAC-ADDRESS>]
```

Description

Shows port security clients status information for the ports. The output can be filtered by interface or MAC address.

Parameter	Description
`all`	Selects all interfaces.
<IF-NAME>	Specifies the interface name.
<MAC-ADDRESS>	Specifies the client MAC address.

Examples

Showing client status information for all ports:

```
switch# show port-access port-security interface all client-status

Port Security Client Status Details

  Authorized-Clients    Type           Port
  ------------------------------------------
  AB:CD:DE:FF:AA:BB     static         1/1/1
  DD:CD:AB:CD:EE:O1     dynamic        1/1/2
  00:50:56:96:7e:fc     sticky-dynamic 1/3/2
```

Showing client status information with sticky-learning enabled for all ports:

```
switch# show port-access port-security interface all client-status

Port Security Client Status Details

  Authorized-Clients    Type              Port
  ---------------------------------------------
  AB:CD:DE:FF:AA:BB     sticky-static     1/1/1
  DD:CD:AB:CD:EE:O1     sticky-dynamic    1/1/2
  DE:CD:AB:BB:EE:O2     sticky-dynamic    1/1/2
```

Showing client status information for a client:

```
switch# show port-access port-security interface 1/3/2 client-status mac
00:50:56:96:7e:fc

Port Security Client Status Details

  Authorized-Clients       Type           Port
  ------------------------------------------------
  00:50:56:96:7e:fc        sticky-dynamic 1/3/2
```

Showing client status information for a port:

```
switch# show port-access port-security interface 1/3/2 client-status

Port Security Client Status Details

  Authorized-Clients       Type           Port
  ------------------------------------------------
  00:50:56:96:7e:fc        sticky-dynamic 1/3/2
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access port-security interface port-statistics

`show port-access port-security interface {all|<IF-NAME>} port-statistics`

Description

Shows port security statistics for the ports in a switch. The output can be filtered by interface.

Parameter	Description
`all`	Selects all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show port-access port-security interface all port-statistics

Port 1/1/1
==========

  Client Details
  --------------
    Number of authorized clients            : 0
    Number of sticky authorized clients     : 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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show port-access security violation sticky-mac-client-move interface

`show port-access security violation sticky-mac-client-move interface {all|<IF-NAME>}`

Description

Shows information about the sticky-mac client move violation. The output can be filtered by interface.

Parameter	Description
`all`	Selects all interfaces.
<IF-NAME>	Specifies the interface name.

Examples

Showing information for all ports.

```
switch# show port-access port-security violation sticky-mac-client-move
        interface all

Sticky MAC Client Move Violation Status Details

-----------------------------------------------------
   Port      Violation      Violation-Count
-----------------------------------------------------
   1/1/1       No                 0
   1/1/2       Yes                10
   1/1/5       No                 10
```

Showing information for a particular port.

```
switch# show port-access port-security violation sticky-mac-client-move
        interface 1/1/1

Sticky MAC Client Move Violation Status Details

-----------------------------------------------------
   Port      Violation      Violation-Count
-----------------------------------------------------
   1/1/1       No                 10
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

sticky-learn enable

```
sticky-learn enable
no sticky-learn enable
```

Description

Enables sticky learning on the port. All the existing and new MACs learned on the port are made sticky.

The **no** form of this command disables the sticky learning on the port.

Examples

Enabling sticky learning on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access port-security
switch(config-if-port-security)# sticky-learn enable
```

Disabling sticky learning on the port:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access port-security
switch(config-if-port-security)# no sticky-learn enable
```

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
6000 6100	`config-if-port-security`	Administrators or local user group members with execution rights for this command.

diag-dump private-vlan basic

```
diag-dump private-vlan basic
```

Description

Collects the debug information in the case of any issue in the PVLAN feature.

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

private-vlan

```
private-vlan {primary | isolated | community} primary-vlan <VLAN-ID>
no private-vlan {primary | isolated | community} primary-vlan <VLAN-ID>
```

Description

Configures a VLAN as either a primary, isolated, or community private VLAN and associates secondary VLANs to a primary VLAN.

The **no** form of this command removes the private VLAN configuration of a VLAN.

Parameter	Description
`primary`	Configures the VLAN as PVLAN type primary. **NOTE:** The number of primary VLANs are restricted to 512

Parameter	Description
	instances for the Aruba 10000 Switch Series. All other switches that support PVLAN support up to 32 primary VLAN instances. Up to 8 secondary VLANs can be configured under a primary VLAN for the Aruba 4100i, 6000, and 6100 Switch Series. Up to 24 secondary VLANs can be configured under a primary VLAN for the Aruba 6200, 6300, 6400, 8325, 8360, and 10000 Switch Series.
`isolated`	Configures the VLAN as PVLAN type isolated.
`community`	Configures the VLAN as PVLAN type community.
<VLAN-ID>	Specifies the primary VLAN ID to be associated. Range: 2-4094.

Examples

Configuring VLAN 100 as PVLAN type primary

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

Removing the private VLAN configuration from VLAN 100

```
switch(config)# vlan 100
switch(config-vlan-100)# no private-vlan primary
```

Associating community VLAN 200 with primary VLAN 100

```
switch(config)# vlan 200
switch(config-vlan-200)# private-vlan community primary-vlan 100
```

Removing the association of community VLAN 200 from primary VLAN 100

```
switch(config)# vlan 200
switch(config-vlan-200)# no private-vlan community primary-vlan 100
```

Associating isolated VLAN 300 with primary VLAN 100

```
switch(config)# vlan 300
switch(config-vlan-300)# private-vlan isolated primary-vlan 100
```

Removing the association of isolated VLAN 300 from primary VLAN 100

```
switch(config)# vlan 300
switch(config-vlan-300)# no private-vlan isolated primary-vlan 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
10.12	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	`config-vlan-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

private-vlan port-type

```
private-vlan port-type {promiscuous | secondary}
no private-vlan port-type {promiscuous | secondary}
```

Description

Configures a port as either promiscuous or secondary when in the **interface** context. Configures PVLAN port type for a role when in the **config-pa-role** context. Multiple secondary VLANs associated with the same primary VLAN cannot be tagged under a secondary port.

The **no** form of this command removes the PVLAN port type configuration.

When an interface has been configured as "vlan trunk allowed all" `private-vlan port-type` cannot be configured.

Parameter	Description
`promiscuous`	Configures the port as promiscuous.
`secondary`	Configures the port as secondary.

Examples

Configuring interface 1/1/1 as promiscuous:

```
switch(config)# interface 1/1/1
switch(config-if)# private-vlan port-type promiscuous
```

Configuring port type as secondary for the port access role:

```
switch(config)# port-access role Role1
switch(config-pa-role)# private-vlan port-type secondary
```

Removing the promiscuous configuration from interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no private-vlan port-type promiscuous
```

Removing port type as secondary for the port access role:

```
switch(config)# port-access role Role1
switch(config-pa-role)# no private-vlan port-type secondary
```

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	`config-if` `config-pa-role`	Administrators or local user group members with execution rights for this command.

show capacities private-vlan

`show capacities private-vlan`

Description

Shows the maximum number of primary and secondary VLANs per domain and secondary ports per LC that can be configured.

Examples

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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 private-vlan

```
show capacities-status private-vlan
```

Description

Shows the number of primary VLANs currently configured and the maximum capacity of primary VLANs on the switch.

Examples

Showing the current capacity status of private-VLAN on the switch

```
switch# show capacities-status private-vlan
System Capacities Status: Filter Private-VLAN
Capacities Status Name                                          Value Maximum
---------------------------------------------------------------------------
Number of Private-VLAN domains currently configured                 2      32
```

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show private-vlan

```
show private-vlan [type {<VLAN-ID> | primary | isolated | community}]
```

Description

Shows the private VLAN configuration for all private VLANs or the private VLAN type specified.

Parameter	Description
<VLAN-ID>	Specifies a list of VLANs. Range: 2-4094.
primary	Shows primary private VLANs.
isolated	Shows isolated private VLANs.
community	Shows community private VLANs.

Examples

Showing all private VLANs

```
switch# show private-vlan
---------------------------------------------
Primary   Isolated          Community
---------------------------------------------
100       201               -
342       -                 1342,3000-3022
343       -                 1343
344       -                 1344
345       -                 1345
```

Showing private VLANs 100 through 102

```
switch# show private-vlan type 100-102
-------------------
VLAN       Type
-------------------
100        Primary
101        Isolated
102        Community
```

Showing all primary VLANs

```
switch# show private-vlan type primary
-------------------
VLAN       Type
-------------------
100        Primary
200        Primary
300        Primary
400        Primary
500        Primary
600        Primary
605        Primary
700        Primary
705        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
10.12	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show private-vlan association

```
show private-vlan association <VLAN-ID>
```

Description

Shows primary and secondary VLAN associations for all private VLANs or a specified private VLAN.

Parameter	Description
<VLAN-ID>	Specifies a list of VLANs. Range: 2-4094.

Examples

Showing all private VLAN associations

```
switch# show private-vlan association
------------------------------------------------
Primary   Isolated   Community
------------------------------------------------
100       101        102,103
200       201        205,210-214
300       301        -
400       -          405-410,411
500       -          502,504,506-508,510,512,514,
                     516,518
600       601,603,   -
605
700       701,703,   707-709,711,713-715,717-719,
          705        721,723-724
```

Showing private VLAN associations for VLAN 100

```
switch# show private-vlan association 100
```

```
--------------------------------------------------
Primary   Isolated   Community
--------------------------------------------------
100       101        102,103
```

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show private-vlan inconsistency

```
show private-vlan inconsistency
```

Description

Shows the list of interfaces and VLANs which are disabled or ignored by private VLAN due to private VLAN configuration and operational inconsistencies.

Possible interface inconsistencies:

- Hardware resource allocation failure
- Interface is a member of multiple secondary VLANs in the same domain
- Interface is a member of both primary and secondary VLAN
- Interface of private vlan port-type promiscuous is not allowed to join secondary VLAN
- Protocol VLANs and private VLANs are mutually exclusive features
- Interface of private vlan port-type secondary is not allowed to join the primary VLAN
- Interface has reached the private-vlan port limit of 24 ports (only applicable for the Aruba 6200 Switch Series)
- Interface is a member of a secondary VLAN which has an SVI configured on it
- Interface **trunk-allowed-all** configuration is not allowed on promiscuous or secondary private-vlan port-type
- VSX ISL configuration is not allowed on private-vlan ports

Possible VLAN inconsistencies:

- Default VLAN is not allowed to join private-vlan domain
- ERPS instances must match for all VLANs in a private-VLAN domain
- VLAN has invalid or no private-vlan primary VLAN association
- MSTP instances must match for all VLANs in a private-VLAN domain
- MVRP and private-VLAN are mutually exclusive features
- VLAN has no primary associated VLAN
- VLAN has reached the private VLAN limit of 32 primary VLANs for the Aruba 4100i, 6000, 6100, 6200, 6300, 6400, 8325, and 8360 Switch Series. (The private VLAN limit is 512 on the Aruba 10000 Switch Series).
- RPVST and private VLAN are mutually exclusive features
- VLAN has reached the private VLAN limit of 24 secondary VLANs on the Aruba 6200, 6300, 6400, 8325, 8360, and 10000 Switch Series or 8 secondary VLANs on the Aruba 4100i, 6000, or 6100 Switch Series.
- Smartlink groups must match for all VLANs in a private-VLAN domain
- VLAN translation and private-VLAN are mutually exclusive features
- VLAN is a secondary VLAN with SVI configured
- Primary VLAN's IGMP snooping configuration is applied
- Primary VLAN's MLD snooping configuration is applied
- Primary VLAN's ND snooping configuration is applied
- Primary VLAN's DHCPV4 snooping configuration is applied
- Primary VLAN's DHCPV6 snooping configuration is applied
- Primary VLAN's CIPT configuration is applied

Examples

Showing interfaces which have been disabled due to private VLAN inconsistencies. In the example below vlan101, vlan201, and vlan301 are secondary VLANs:

```
switch# show private-vlan inconsistency
------------------------------------------------------------------------
Interface/VLAN   Action    Inconsistency-Reason
------------------------------------------------------------------------
1/1/1            Down      Interface is a member of multiple secondary VLANs
1/2/5            Down      Interface is a member of both primary and secondary
VLAN
vlan20           Down      VLAN has invalid or no private-vlan primary VLAN
association
vlan101          Ignore    Primary VLAN's IGMP snooping config is applied.
vlan201          Ignore    Primary VLAN's ND snooping config is applied.
vlan301          Ignore    Primary VLAN's DHCPV4 snooping config is applied.
```

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show private-vlan port-type

```
show private-vlan port-type
```

Description

Shows all the private VLAN port type configurations.

Examples

Showing the ports with private-vlan port-type configuration

```
switch# show private-vlan port-type
-------------------------------------------------
Port            Port Type
-------------------------------------------------
1/1/1           promiscuous
1/1/2           secondary
```

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators 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-configuration private-vlan

```
show running-configuration private-vlan
```

Description

Shows all private VLAN configurations on the switch.

Examples

Showing the current private VLAN configuration

```
switch# show running-configuration private-vlan
vlan 300
private-vlan type primary
vlan 100
private-vlan type isolated primary-vlan 300
vlan 200
private-vlan type community primary-vlan 300
interface 1/1/1
vlan trunk allowed 300
private-vlan port-type promiscuous
interface 1/1/2
vlan trunk allowed 100
private-vlan port-type secondary
interface 1/1/3
vlan trunk allowed 200
private-vlan port-type secondary
`````
```

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 | Command introduced for 4100i, 6000, 6100, and 8100 Switch series |

### Command Information

| Platforms | Command context | Authority |
|---|---|---|
| 6000<br>6100 | Operator (>) or Manager (#) | Operators 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 private-vlan

```
show tech private-vlan
```

Description

Shows the output of **show tech** for the private-VLAN feature.

Example
```

Showing the output of **show tech** for private-VLAN

```
switch# show tech private-vlan
==================================================
Show Tech executed on Mon Sep 28 06:05:02 2020
==================================================
==================================================
[Begin] Feature private-vlan
==================================================
*********************************
Command : show running-config private-vlan
*********************************
vlan 100
private-vlan primary
vlan 101
private-vlan isolated primary-vlan 100
vlan 102
private-vlan community primary-vlan 100
vlan 200
private-vlan primary
vlan 201
private-vlan community primary-vlan 200
interface 1/1/1
vlan access 1
private-vlan promiscuous
interface 1/1/2
vlan access 1
private-vlan secondary
*********************************
Command : show private-vlan type
*********************************
--------------------
VLAN      Type
--------------------
100       primary
101       isolated
102       community
200       primary
201       community
*********************************
Command : show private-vlan association
*********************************
-------------------------------------------
Primary   Isolated          Community
-------------------------------------------
100       101               102
200       -                 201
*********************************
Command : show private-vlan port-type
*********************************
----------------------
Port      Port-type
----------------------
1/1/1     promiscuous
1/1/2     secondary
==================================================
[End] Feature private-vlan
==================================================
==================================================
```

```
Show Tech commands executed successfully
================================================
```

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	Command introduced for 4100i, 6000, 6100, and 8100 Switch series

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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.

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 CoS values 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.

- Queues must be consecutively defined starting at queue number zero. For example, a four-queue profile with priority values defined for queues 0, 1, 2, 3 is valid, but a four-queue profile which defines priority values for queues 1, 3, 5, and 7 is not.
- There can be only 2, 4, or 8 queues in a queue profile configuration and the queues must be consecutively numbered starting at zero.
- All queues must use the same algorithm except for the highest numbered queue, which may be strict.

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:

Examples

The following commands illustrate a valid configuration where every CoS value is assigned to a queue and all assigned queues are defined:

```
switch(config)# qos trust cos
switch(config)# qos queue-profile Q1
switch(config)# map queue 0 cos 0
switch(config)# map queue 1 cos 1
switch(config)# map queue 2 cos 2
switch(config)# map queue 3 cos 3
switch(config)# map queue 4 cos 4
switch(config)# map queue 5 cos 5
switch(config)# map queue 6 cos 6
switch(config)# map queue 7 cos 7
switch(config)# qos schedule-profile S1
switch(config)# min-bandwidth queue 0 percent 5
switch(config)# min-bandwidth queue 1 percent 5
switch(config)# min-bandwidth queue 2 percent 10
switch(config)# min-bandwidth queue 3 percent 10
switch(config)# min-bandwidth queue 4 percent 20
switch(config)# min-bandwidth queue 5 percent 20
switch(config)# min-bandwidth queue 6 percent 10
switch(config)# min-bandwidth queue 7 percent 20
```

The following commands illustrate an invalid configuration because CoS 2 is not assigned to a queue:

```
switch(config)# qos trust cos
switch(config)# qos queue-profile Q1
switch(config)# map queue 0 cos 0
switch(config)# map queue 1 cos 1
switch(config)# map queue 3 cos 3
switch(config)# map queue 4 cos 4
switch(config)# map queue 5 cos 5
switch(config)# map queue 6 cos 6
switch(config)# map queue 7 cos 7
switch(config)# qos schedule-profile S1
switch(config)# min-bandwidth queue 0 percent 5
switch(config)# min-bandwidth queue 1 percent 5
switch(config)# min-bandwidth queue 3 percent 10
switch(config)# min-bandwidth queue 4 percent 20
switch(config)# min-bandwidth queue 5 percent 20
switch(config)# min-bandwidth queue 6 percent 10
switch(config)# min-bandwidth queue 7 percent 20
```

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.

map queue

```
map queue <QUEUE-NUMBER> cos <PRIORITY-NUMBER>
no map queue <QUEUE-NUMBER> [cos <PRIORITY-NUMBER>]
```

Description

Assigns a CoS value to a queue in a queue profile. By default, the larger the queue number the higher its priority. A queue without a CoS value assigned to it is not used to store packets. The same queue can be assigned multiple CoS values.

The **no** form of this command removes the specified cos value from a specific queue. If no CoS value is specified, then all CoS values are removed from the queue.

Parameter	Description
<QUEUE-NUMBER>	Specifies the queue number. Range: 0 to 7.
<PRIORITY-NUMBER>	Specifies the CoS value. Range: 0 to 7, where 0 is the lowest priority and 7 is the highest.

Usage

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.

min-bandwidth

```
min-bandwidth queue <QUEUE-NUMBER> percent <PERCENTAGE>
no min-bandwidth queue <QUEUE-NUMBER>
```

Description

Assigns the Guaranteed Minimum Bandwidth (GMB) algorithm and a percentage of bandwidth to a queue. GMB allocates available bandwidth among all non-empty queues in relation to their configured minimum bandwidth. Non-empty queues are serviced first in strict order up to their minimum bandwidth. If there is any remaining bandwidth, the scheduler will strictly service any remaining non-empty queues.

The **no** form of this command only clears the algorithm for a queue if GMB has been assigned.

Occasionally, the following errors may occur:

- *The schedule profile total sum of GMB percentages must not exceed 100.*

This error occurs when attempting to apply a schedule profile with sum of GMB percentages of queues exceed 100 percentage. The solution is to configure GMB perecntage for queues, so that the sum of percentage must not exceed 100.

Parameter	Description
<QUEUE-NUMBER>	Specifies the queue number. Range: 0 to 7.
<PERCENTAGE>	Specifies bandwidth percentage used for GMB scheduling. Range: 0 to 100.

Examples

Assigning queue **0** of schedule profile **S1** the GMB scheduling algorithm with minimum bandwidth of **5 percent**:

```
switch(config)# qos schedule-profile S1
switch(config-schedule)# min-bandwidth queue 0 percent 5
```

Removing GMB from queue 0:

```
switch(config)# qos schedule-profile s1
switch(config-schedule)# no min-bandwidth queue 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
6000 6100	config-schedule-*<NAME>*	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

```
qos cos <CODE-POINT>
no qos cos
```

Description

Configures a CoS PCP remark for an Ethernet or LAG interface. Packets that ingress on the interface are remarked at egress using the configured CoS PCP value.

The remark only occurs when QoS trust mode on the interface is set to **none**.

If QoS trust mode is not set to **none**, then the remark is ignored, and the following commands will show the CoS remark status as **ignored (incompatible Port Access Trust configuration**) or **not applied' (incompatible QoS global/port Trust configuration)**:

- show running-configuration
- show interface <*PORT-NUM*>
- show interface <*PORT-NUM*> qos

The **no** form of this command removes a CoS remark on an interface.

Parameter	Description
<CODE-POINT>	Specifies an 802.1 VLAN priority CoS value. Range: 0 to 7.

Examples

Configuring a CoS remark of **3** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# qos trust none
switch(config-if)# qos cos 3
```

Deleting a CoS remark of **3** on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no qos cos
```

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
6000 6100	config-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 *ignored* (incompatible Port Access Trust configuration) or *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. The CoS metadata is assigned from the DSCP map entry indexed by the DSCP remark value.
2. If a CoS remark is also configured along with the DSCP remark, the CoS remark value will be assigned to the packet's CoS metadata.
3. The CoS metadata and queue profile are then used to determine the queue for the packet. If the packet is transmitted with an 802.1Q VLAN tag, the PCP will be remarked to match the CoS metadata.

For arriving non-IP packets:

The CoS metadata is assigned from the DSCP map entry indexed by the DSCP remark value. This CoS value and the queue profile are used to select the queue for packet scheduling. The PCP of tagged non-IP packets will be remarked to this CoS value.

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
6000 6100	`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>  [color <COLOR>] [cos <COS-VALUE>] [name <DESCRIPTION>]
no qos dscp-map <CODE-POINT>
```

Description

Defines the CoS value 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.

The color <*COLOR*> parameter is supported only in 4100i Switch Series.

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
DSCP     code_point cos  name
-------- ---------- ---  ----
000000   0          0    CS0
000001   1          0
000010   2          0
000011   3          0
000100   4          0
000101   5          0
...
101101   45         5
101110   46         5    EF
101111   47         5
110000   48         6    CS6
...
111100   60         7
111101   61         7
111110   62         7
111111   63         7
```

Parameter	Description
<CODE-POINT>	Specifies an IP differentiated services code point. Range: 0 to 63. Default: 0.
`cos` *<COS-VALUE>*	Specifies an 802.1p VLAN priority CoS remark value. Range: 0 to 7. Default 0.
`cos` *<PCP-VALUE>*	Specifies an optional 802.1p VLAN Priority Code Point remark value. Range: 0 to 7. Default: No remark.
`name` *<DESCRIPTION>*	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

```
switch(config)# qos dscp-map 46 cos 7 name new color yellow
```

Setting code point **41** to a CoS of **6**:

```
switch(config)# qos dscp-map 41 cos 6
```

Setting code point **41** to the default value:

```
switch(config)# no qos dscp-map 41
```

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
6000 6100	`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 CoS values. Each profile has two, four, or 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     percent max-bandwidth_kbps
--------- ------------- ------- ------------------
0         min-bandwidth 2
1         min-bandwidth 3
2         min-bandwidth 30
3         min-bandwidth 10
4         min-bandwidth 10
5         min-bandwidth 10
6         min-bandwidth 15
7         min-bandwidth 20
```

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, GMB).
2. The highest queue number uses strict priority, and all remaining (lower) queues use the same algorithm (for example, GMB). This supports priority scheduling behavior necessary for the IEFT RFC 3246 Expedited Forwarding specification (https://tools.ietf.org/html/rfc3246).

Only limited changes can be made to an applied schedule profile:

- The percentage of a GMB queue.
- The bandwidth of a strict queue or a min-bandwidth queue.
- The algorithm of the highest numbered queue can be swapped between GMB 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 trust

```
qos trust {none|cos|dscp}
no qos trust
```

Description

Configures one of three modes that are applied globally on all Ethernet interfaces and LAGs that have not applied their own trust mode. Trust mode determines whether VLAN or IP headers are used to assign CoS

values to ingress packets.

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 CoS value zero.
cos	For 802.1 VLAN-tagged packets, use the priority code point field from the outermost VLAN header to assign the CoS value. For untagged packets, the CoS value is assigned to zero. Default.
dscp	For IP packets, use the DSCP as the index into the DSCP Map table to obtain the CoS value for the packet. For non-IP packets, the CoS value is assigned to zero.

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
```

WARNING: QoS port remark configurations are not applied when the QoS trust mode is *mode*. This warning message 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*.

WARNING: QoS port remark configurations are not applied when the global QoS trust mode is *mode*. This warning message 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.

rate-limit

```
rate-limit {broadcast|multicast|unknown-unicast|icmp {ip-all|ip|ipv6}} <RATE>
{kbps|percent}
no rate-limit {broadcast|multicast|unknown-unicast|icmp}
```

Description

Sets the amount of traffic of a specific type that can ingress on an Ethernet interface, 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 **no** form of this command removes the traffic limit for the specified traffic type.

Parameter	Description
`{broadcast|multicast|unknown-unicast|icmp {ip-all|ip|ipv6}}`	Specifies the type of ingress traffic to which the rate limit applies: broadcast, multicast, unknown-unicast, or ICMP. 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. Unknown-unicast packets may be intended for devices whose addresses have temporarily aged out of network forwarding caches. Configuring rate limits can help provide balance between necessary and flooded traffic. The ICMP rate limit can be configured to apply to IPv4, IPv6, or all IP traffic. Only one ICMP rate-limit can be configured at a time. Applying a new ICMP rate-limit replaces any previous ICMP rate-limit.
`<RATE> {kbps|percent}`	Specifies the rate limit in kilobits-per-second or as a percentage of link bandwidth. Range: 64 to 10000000 kbps

Parameter	Description
	(in steps of 64 kbps), or 1-100 percent. The actual rate limit will be approximately equivalent to the minimum of the two 64-kbps step values that are closest to the configured (or kbps-converted) 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.

Examples

Limiting broadcast traffic to **1024kbps** on interface **1/1/3**:

```
switch(config)# interface 1/1/3
switch(config-if)# rate-limit broadcast 1024 kbps
```

Limiting all ICMP IPv4 traffic to **1024kbps** on interface **1/1/3**:

\\\\\\

```
switch(config)# interface 1/1/3
switch(config-if)# rate-limit icmp ip 1024 kbps
```

Configuring a multicast rate-limit as a percentage of link bandwidth:

```
switch(config)# interface 1/1/3
switch(config-if)# rate-limit multicast 1 percent
```

Viewing the results of the previous configuration settings:

```
switch# show interface 1/1/3 qos
Interface 1/1/3 is up
 Admin state is up
 qos trust cos (global)
 qos queue-profile factory-default (global)
 qos schedule-profile factory-default (global)
 rate-limit unknown-unicast 1024 kbps (1024 actual)
 rate-limit broadcast 1024 kbps (1100 actual)
 rate-limit multicast 1 percent (10000 actual)
 rate-limit icmp ip-all 1024 kbps (1024 actual)

switch# show interface 1/1/3

Interface 1/1/3 is up
 Admin state is up
 Link state: up for 3 minutes (since Thu Nov 26 17:56:14 UTC 2020)
 Link transitions: 1
 Description:
 Hardware: Ethernet, MAC Address: f8:60:f0:c9:21:bc
 MTU 1500
 Type 1GbT
 Full-duplex
 qos trust cos
 rate-limit unknown-unicast 1024 kbps (1024 actual)
 rate-limit broadcast 1024 kbps (1100 actual)
 rate-limit multicast 1 percent (10000 actual)
 rate-limit icmp ip-all 1024 kbps (1024 actual)
 Speed 1000 Mb/s
 Auto-negotiation is on
 Energy-Efficient Ethernet is disabled
 Flow-control: off
 Error-control: off
 MDI mode: MDIX
 VLAN Mode: access
 Access VLAN: 1
 Rx
            0 total packets                   0 total bytes
            0   unicast packets
            0   multicast packets
            0   broadcast packets
            0 errors                          0 dropped
            0 CRC/FCS                         0 pause
```

```
Tx
     1057962 total packets            366066962 total bytes
           0   unicast packets
           0   multicast packets
     1058039   broadcast packets
           0 errors                           0 dropped
           0 collision                        0 pause
```

For more information on features that use this command, refer to the Quality of Service Guide for your switch model.

Command History

Release	Modification
10.14	Replaced the **ipv4** parameter with the **ip** parameter. The **ipv4** parameter is deprecated.
10.13	Added percent parameter.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`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. The byte count includes any packets subsequently dropped by an egress ACL .

- **Tx Packets:** Total packets transmitted. The count includes packets subsequently dropped by an egress ACL .
- **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 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 up
 Admin state is up
 qos trust cos (global)
 qos queue-profile factory-default (global)
 qos schedule-profile factory-default (global)
 qos cos 5
 qos dscp 47
 rate-limit unknown-unicast 1 percent (10000 actual)
 rate-limit broadcast 40000 kbps (40000 actual)
 rate-limit icmp ip-all 10000 kbps (10000 actual)
```

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 dscp-map

`show qos dscp-map [default]`

Description

Displays the current or default global QoS dscp-map.

Parameter	Description
`default`	Shows the factory default DSCP code point settings.

Examples

Showing the current QoS DSCP map:

```
switch# show qos dscp-map
DSCP     code_point cos  name
-------- ---------- ---  ----
000000   0          0    CS0
000001   1          0
000010   2          0
000011   3          0
000100   4          0
000101   5          0
...
101101   45         5
101110   46         6    new
101111   47         5
110000   48         6    CS6
...
111101   61         7
111110   62         7
111111   63         7
```

Showing the default QoS DSCP map:

```
switch# show qos dscp-map default
DSCP     code_point cos  name
-------- ---------- ---  ----
000000   0          0    CS0
000001   1          0
000010   2          0
000011   3          0
000100   4          0
000101   5          0
...
101101   45         5
101110   46         5
101111   47         5
110000   48         6    CS6
...
111100   60         7
111101   61         7
111110   62         7
111111   63         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 queue-profile

`show qos queue-profile [<NAME> | factory-default]`

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.

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 cos values must be mapped to some queue.
- There can be only 2, 4, or 8 queues.
- The queues must be consecutively numbered starting at zero.

Examples

Showing the settings of the factory default queue profile:

```
switch# show qos queue-profile factory-default
queue_num cos name
--------- --- ----
0         1
1         0
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]`

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.

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                                 Maximum   Bandwidth
Number  Algorithm      Percent   Bandwidth   Units
------- -------------- -------- ----------   ----------
0       min-bandwidth  2
1       min-bandwidth  3
2       min-bandwidth  30
3       min-bandwidth  10
4       min-bandwidth  10
5       min-bandwidth  10
6       min-bandwidth  15
7       min-bandwidth  20
```

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 trust

```
show qos trust [default]
```

Description

Shows the global QoS trust settings, or the factory default settings.

Parameter	Description
`default`	Shows the factory default QoS trust settings.

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 cos
```

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.

strict queue

```
strict queue <0-7> [max-bandwidth <RATE> [kbps|percent]
no strict queue <0-7> [max-bandwidth <RATE> [kbps|percent]
```

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** option to limit the amount of traffic transmitted per output queue. 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.

The **no** form of this command removes the queue configuration from the schedule profile. To remove only egress queue shaping, re-enter the strict queue command without the **max-bandwidth** parameter.

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: 468 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.

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 *min-bandwith*

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:

```
switch(config)# qos schedule-profile MySchedule
```

```
switch(config-schedule)# strict queue 7 max-bandwidth 10000 kbps
```

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-<NAME>`	Administrators or local user group members with execution rights for this command.

Chapter 78
Configurable RADIUS attribute commands

aaa radius-attribute group

```
aaa radius-attribute group <GROUP-NAME>
no aaa radius-attribute group <GROUP-NAME>
```

Description

Configures an existing RADIUS server group for which the configured RADIUS attributes will be included in request packets. Enters the **config-radius-attr** context.

The **no** form of this command unconfigures the RADIUS server group for the configured RADIUS attributes.

Nas-id and tunnel-private-group-id attributes only apply to port access requests. Nas-ip-addr attributes only apply to management user requests.

Parameter	Description
<GROUP-NAME>	Specifies an existing RADIUS server group name.

Examples

Configuring port access request RADIUS attributes for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-id value ARUBA_NAS-01
switch(config-radius-attr)# nas-id request-type authentication
switch(config-radius-attr)# tunnel-private-group-id value static
switch(config-radius-attr)# tunnel-private-group-id request-type authentication
```

Configuring management user request RADIUS attributes for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# nas-ip-addr request-type authentication
switch(config-radius-attr)# nas-ip-addr service-type user-management
```

Unconfiguring RADIUS attributes for **rad_group1**:

```
switch(config)# no aaa radius-attribute group rad_group1
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

nas-id request-type

```
nas-id request-type {authentication | accounting | both}
no nas-id request-type {authentication | accounting | both}
```

Description

For the selected (by context) RADIUS server group, configures the Network Access Server (NAS) ID request type for which the attribute configured with command **nas-id value** will be included.

The no form of this command unconfigures the specified request type.

Nas-id attributes only apply to port access requests.

Parameter	Description
`authentication`	Selects the authentication request type.
`accounting`	Selects the accounting request type.
`both`	Selects both the authentication and accounting request types.

Examples

Configuring the authentication request type for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-id request-type authentication
```

Configuring both the authentication and accounting request types for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# nas-id request-type both
```

Unconfiguring the authentication request type for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-id request-type 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
6000 6100	`config-radius-attr`	Administrators or local user group members with execution rights for this command.

nas-id value

```
nas-id value <NAS-ID>
no nas-id [value <NAS-ID>]
```

Description

For the selected (by context) RADIUS server group, configures the Network Access Server Identifier (NAS ID) (type 32, RFC 2865). The NAS ID is sent in the RADIUS access request and accounting packets to notify the source of the RADIUS access request.

The **no** form of this command unconfigures the specified NAS ID.

Nas-id attributes only apply to port access requests.

Parameter	Description
<NAS-ID>	Specifies the FQDN or other unique identifying name of the Network Access Server (NAS). Range 1 to 253 characters.

Examples

Configuring the Network Access Server (NAS) ID for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-id value ARUBA_NAS-01
```

Unconfiguring the NAS ID for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-id value ARUBA_NAS-01
```

Unconfiguring both the NAS-ID value and the request type for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# no nas-id
```

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
6000 6100	`config-radius-attr`	Administrators or local user group members with execution rights for this command.

nas-ip-addr request-type authentication

```
nas-ip-addr request-type authentication
no nas-ip-addr request-type authentication
```

Description

For the selected (by context) RADIUS server group, configures the **NAS-IP-Address** attribute for inclusion in management user request packets.

The no form of this command unconfigures the **NAS-IP-Address** attribute for inclusion in management user request packets.

Nas-ip-addr attributes only apply to management user requests.

Examples

Configuring the **NAS-IP-Address** attribute for inclusion in management user request packets for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-ip-addr request-type authentication
```

Unconfiguring the **NAS-IP-Address** attribute for inclusion in management user request packets for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-ip-addr request-type authentication
```

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

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config-radius-attr`	Administrators or local user group members with execution rights for this command.

nas-ip-addr service-type user-management

```
nas-ip-addr service-type user-management
no nas-ip-addr service-type user-management
```

Description

For the selected (by context) RADIUS server group, configures the **NAS-IP-Address** attribute for inclusion in management user service type request packets.

The no form of this command unconfigures the **NAS-IP-Address** attribute for inclusion in management user service type request packets.

Nas-ip-addr attributes only apply to management user requests.

Examples

Configuring the **NAS-IP-Address** attribute for inclusion in management user service type request packets for **rad_group1:**

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# nas-ip-addr service-type user-management
```

Unconfiguring the **NAS-IP-Address** attribute for inclusion in management user service type request packets for **rad_group1:**

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no nas-ip-addr service-type user-management
```

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

Command History

Release	Modification
10.09	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config-radius-attr`	Administrators or local user group members with execution rights for this command.

tunnel-private-group-id request-type

```
tunnel-private-group-id request-type {authentication | accounting | both}
no tunnel-private-group-id request-type {authentication | accounting | both}
```

Description

For the selected (by context) RADIUS server group, configures the request type for which the attribute configured with command **tunnel-private-group-id value** will be included.

The **no** form of this command unconfigures the specified request type.

Tunnel-private-group-id attributes only apply to port access requests.

Parameter	Description
`authentication`	Selects the authentication request type.
`accounting`	Selects the accounting request type.
`both`	Selects both the authentication and accounting request types.

Examples

Configuring the authentication request type for **rad_group1**:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# tunnel-private-group-id request-type authentication
```

Configuring both the authentication and accounting request types for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# tunnel-private-group-id request-type both
```

Unconfiguring the authentication request type for **rad_group2**:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# no tunnel-private-group-id request-type 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
6000 6100	`config-radius-attr`	Administrators or local user group members with execution rights for this command.

tunnel-private-group-id value

```
tunnel-private-group-id value {static | dynamic}
no tunnel-private-group-id value {static | dynamic}
```

Description

For the selected (by context) RADIUS server group, configures the **tunnel-private-group-id** value (type 81, RFC 2868) that will be sent in RADIUS access-request packets. This is used for VLAN identification.

The no form of this command unconfigures specified **tunnel-private-group-id** value.

Tunnel-private-group-id attributes only apply to port access requests.

Parameter	Description
`static`	Causes the switch to send (as an attribute value) the native VLAN of the client port.
`dynamic`	Causes the switch to send (as an attribute value) the client VLAN assigned by server. This is applicable during re-authentication scenarios.

Examples

Configuring **rad_group1** for the RADIUS attribute to identify the native VLAN of the client port:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# tunnel-private-group-id value static
```

Configuring **rad_group2** for the RADIUS attribute to identify the client VLAN assigned by the server:

```
switch(config)# aaa radius-attribute group rad_group2
switch(config-radius-attr)# tunnel-private-group-id value dynamic
```

Unconfiguring (for **rad_group1**) the RADIUS attribute to identify the native VLAN of the client port:

```
switch(config)# aaa radius-attribute group rad_group1
switch(config-radius-attr)# no tunnel-private-group-id value static
```

Unconfiguring (for **rad_group3**) both the group-ID value and request type:

```
switch(config)# aaa radius-attribute group rad_group3
switch(config-radius-attr)# no tunnel-private-group-id
```

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
6000 6100	`config-radius-attr`	Administrators or local user group members with execution rights for this command.

Chapter 79
RADIUS dynamic authorization commands

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

radius dyn-authorization enable

```
radius dyn-authorization enable
no radius dyn-authorization enable
```

Description

Enables RADIUS dynamic authorization. This command must be issued before the configuration set with other **radius dyn-authorization** commands takes effect.

The no form of this command disables RADIUS dynamic authorization.

Examples

Enabling RADIUS dynamic authorization:

```
switch(config)# radius dyn-authorization enable
```

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
6000 6100	config	Administrators or local user group members with execution rights for this command.

radius dyn-authorization client

```
radius dyn-authorization client {<IPV4> | <IPV6> | <HOSTNAME>}
   [secret-key [plaintext <PASSKEY> | ciphertext <PASSKEY>]]
   [time-window <WIDTH>] [vrf <VRF-NAME>] [replay-protection {enable|disable}]
   [rfc5176-enforcement-mode <strict|loose>]
   no...
```

Description

Configures RADIUS dynamic authorization for the specified client on the specified (or **default**) VRF.

The **no** form of this command unconfigures RADIUS dynamic authorization for the specified client on the specified (or **default**) VRF.

Guidelines

Configure **rfc5176-enforcement-mode loose** when integrating with the Adaptive Network Control (ANC) feature of Cisco ISE, as authorization attributes are sent as part of Disconnect-Requests (code 40) instead of CoA-Requests(code 43).

The following are the only authorization attributes that are accepted in the disconnect requests in the loose mode:

1. Cisco-AVPair='subscriber:command=bounce-host-port'
2. Cisco-AVPair='subscriber:command=disable-host-port'
3. Cisco-AVPair='subscriber:command=reauthenticate' and Cisco-AVPair='subscriber:reauthenticate-type=<last|rerun>

The **reauthenticate-type=rerun** option is not supported if concurrent onboarding is enabled for the client.

Parameter	Description
<IPV4> | *<IPV6>* | *<HOSTNAME>*	Specifies the client IPv4 address, IPv6 address, or host name.
`secret-key [plaintext` *<PASSKEY>* | `ciphertext` *<PASSKEY>*`]`	Specifies the dynamic authorization server (RADIUS server) shared secret key required for client access. Provide either a plaintext or an encrypted shared-secret passkey. As per RFC 2865, the shared-secret can be a mix of alphanumeric and special characters. Plaintext passkeys are between 1 and 32 alphanumeric and special characters. **NOTE:** When **secret-key** is entered without either sub-parameter, plaintext shared secret prompting occurs upon pressing Enter. Enter must be pressed immediately after the **secret-key** parameter without entering other parameters. The entered shared secret characters are masked with asterisks.
`rfc5176-enforcement-mode <strict|loose)`	Configure the enforcement mode of RFC5176. The default mode is **strict** and in this mode, no authorization attributes are allowed as part of disconnect requests. When configured mode is **loose**, then the authorization attributes are accepted in disconnect requests.
`time-window` *<WIDTH>*	Specifies the width of the synchronization window (in seconds) between the RADIUS dynamic authorization client and the RADIUS dynamic authorization server. Default 300. Range: 1 to 65535.
`replay-protection {enable|disable}`	Enables or disables RADIUS dynamic authorization replay protection for the specified client on the specified (or **default**) VRF. By default, the replay-

Parameter	Description
	protection is set to disabled.
`vrf <VRF-NAME>`	Specifies the VRF on which the identified client is connected. When omitted, VRF **default** is assumed.

Examples

Configuring RADIUS dynamic authorization with replay protection for a client on the default VRF:

```
switch(config)# radius dyn-authorization client 1.1.2.5 replay-protection enable
```

Configuring RADIUS dynamic authorization with time window and shared secret for a client on the default VRF:

```
switch(config)# radius dyn-authorization client 1.1.2.7 time-window 8
                secret-key plaintext skF82#450
```

Configuring loose enforcement of RFC5176:

```
switch(config)# radius dyn-authorization client 1.1.1.1 rfc5176-enforcement-mode
loose
```

Configuring RADIUS dynamic authorization with a prompted shared secret:

```
switch(config)# radius dyn-authorization client 1.1.2.7 secret-key
Enter the RADIUS dyn-authorization key: *********
Re-Enter the RADIUS dyn-authorization key: *********
```

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

Command History

Release	Modification
10.13	The **rfc5176-enforcement-mode** parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

radius dyn-authorization client tls (RadSec)

```
radius dyn-authorization client [<IPV4> | <IPV6> | <HOSTNAME>]
   tls [replay-protection {enable|disable}][time-window <WIDTH>] [vrf <VRF-NAME>]
[rfc5176-enforcement-mode <strict|loose>]
no radius dyn-authorization client [<IPV4> | <IPV6> | <HOSTNAME>]
   tls [replay-protection {enable|disable}][time-window <WIDTH>] [vrf <VRF-NAME>]
[rfc5176-enforcement-mode <strict|loose>]
```

Description

Enables TLS protection for a RADIUS dynamic authorization client on the specified (or **default**) VRF. RadSec is a protocol that supports RADIUS over TLS. The **no** form of this command deletes TLS protection for the dynamic authorization client.

RadSec server must be configured before configuring dynamic authorization.

Guidelines

Configure **rfc5176-enforcement-mode loose** when integrating with the Adaptive Network Control (ANC) feature of Cisco ISE, as authorization attributes are sent as part of Disconnect-Requests (code 40) instead of CoA-Requests(code 43).

The following are the only authorization attributes that are accepted in the disconnect requests in the loose mode:

1. Cisco-AVPair='subscriber:command=bounce-host-port'
2. Cisco-AVPair='subscriber:command=disable-host-port'
3. Cisco-AVPair='subscriber:command=reauthenticate' and Cisco-AVPair='subscriber:reauthenticate-type=<last|rerun>

The **reauthenticate-type=rerun** option is not supported if concurrent onboarding is enabled for the client.

Parameter	Description
`<IPV4> | <IPV6> | <HOSTNAME>`	Specifies the client IPv4 address, IPv6 address, or host name.
`replay-protection {enable|disable}`	Enables or disables RADIUS dynamic authorization replay protection for the specified client on the specified (or **default**) VRF. By default, the replay-protection is set to disabled.
`time-window <WIDTH>`	Specifies the width of the synchronization window (in seconds) between the RADIUS dynamic authorization client and the RADIUS dynamic authorization server. Default 300. Range: 1 to 65535.
`vrf <VRF-NAME>`	Specifies the VRF on which the identified client is connected. When omitted, VRF **default** is assumed.
`rfc5176-enforcement-mode <strict|loose>`	Configure the enforcement mode of RFC5176. The default mode is **strict** and in this mode, no authorization attributes are allowed as part of disconnect requests. When configured mode is **loose**, then the authorization attributes are accepted in disconnect requests.

Examples

Enables TLS protection for a RADIUS dynamic authorization client with replay protection and time window for a client on the default VRF:

```
switch(config)# radius dyn-authorization client 1.1.2.5 tls replay-protection
enable time-window 8
```

Configuring loose enforcement of RFC5176:

```
switch(config)# radius dyn-authorization client 1.1.1.1 tls rfc5176-enforcement-
mode loose
```

Deleting TLS protection for a dynamic authorization client on the adm2 VRF:

```
switch(config)# no radius dyn-authorization client 1.1.2.7 tls VRF adm2
```

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

Command History

Release	Modification
10.13	The **rfc5176-enforcement-mode** parameter was introduced.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	config	Administrators or local user group members with execution rights for this command.

radius dyn-authorization port

radius dyn-authorization port *<PORT-NUMBER>*

Description

Sets the RADIUS dynamic authorization server UDP or TCP port.

Parameter	Description
<PORT-NUMBER>	Specifies the UDP or TCP port. Default UDP: 3799 and TCP:2083.

Examples

Setting the RADIUS dynamic authorization server UDP port back to its default 3799:

```
switch(config)# radius dyn-authorization port 3799
```

Setting the RADIUS dynamic authorization server TCP port back to its default 2083:

```
switch(config)# radius dyn-authorization port 2083
```

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
6000 6100	config	Administrators or local user group members with execution rights for this command.

show radius dyn-authorization

```
show radius dyn-authorization
```

Description

Shows RADIUS dynamic authorization configuration and summarized statistics for all clients configured for dynamic authorization.

Usage

Show command output item identification:

- **Radius Dynamic Authorization**: Enabled or Disabled status, system wide.
- **Radius Dynamic Authorization Port**: The UDP or TCP port used for dynamic authorization (default 3799).
- **Invalid Client Address in CoA Requests**: The number of CoA (change of authorization) requests received with an incorrect DAC (dynamic authorization client) address.
- **Invalid Client Address in Disconnect Requests**: The number of disconnect requests received with incorrect DAC address.
- **Disconnect Requests**: The number of disconnect requests received from the DAC.
- **Disconnect ACKs**: The number of Disconnect-ACKs sent to the DAC.
- **Disconnect NAKs**: The number of Disconnect-NAKs sent to the DAC.
- **CoA Requests**: The number of CoA-requests received from the DAC.
- **CoA ACKs**: The number of CoA-ACKs sent to the DAC.
- **CoA NAKs**: The number of CoA-NAKs sent to the DAC.

Example

Showing RADIUS dynamic authorization summarized statistics for all clients configured for dynamic authorization:

```
switch# show radius dyn-authorization
Status and Counters - RADIUS Dynamic Authorization Information

  RADIUS Dynamic Authorization                   : Enabled
  RADIUS Dynamic Authorization UDP Port          : 3799
  Invalid Client Addresses in CoA Requests       : 0
  Invalid Client Addresses in Disconnect Requests: 0

Dynamic Authorization Client Information
========================================

IP Address          : 1.1.2.1
VRF                 : adm2
Replay Protection   : Disabled
TLS Enabled         : Yes
Time Window         : 20
Disconnect Requests : 1
Disconnect ACKs     : 1
Disconnect NAKs     : 0
CoA Requests        : 7
CoA ACKs            : 2
CoA-NAKs            : 5
Shared-Secret       :
AQBapb+HsdpqV1Q3CPCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOwZSNzA2SWrLA=


IP Address          : 1.1.2.5
VRF                 : default
Replay Protection   : Enabled
TLS Enabled         : No
Time Window         : 20
Disconnect Requests : 6
Disconnect ACKs     : 6
Disconnect NAKs     : 0
CoA Requests        : 9
CoA ACKs            : 5
CoA-NAKs            : 4
Shared-Secret       :
AQBapb+HsdpqV1Q3CPCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOwZSNzA2SWrLA=


IP Address          : 1.1.2.7
VRF                 : default
Replay Protection   : Disabled
TLS Enabled         : Yes
Time Window         : 8
Disconnect Requests : 6
Disconnect ACKs     : 6
Disconnect NAKs     : 0
CoA Requests        : 9
CoA ACKs            : 5
CoA-NAKs            : 4
Shared-Secret       :
AQBapb+HsdpqV1Q3CPCBMQTG8ekK1cA+CyD0RvfbeA8BEgikCgAAAJOwZSNzA2SWrLA=
```

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
6000 6100	Operator (>) or Manager (#)	Operators 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 dyn-authorization client

`show radius dyn-authorization client <IP-ADDR> [vrf <VRF-NAME>]`

Description

Shows RADIUS dynamic authorization statistics for the specified client on the specified VRF.

Parameter	Description
<IP-ADDR>	Specifies the client IPv4 or IPv6 address.
`vrf` *<VRF-NAME>*	Specifies the VRF on which the identified client is connected. When omitted, VRF **default** is assumed.

Usage

Show command output item identification:

- **Total Requests**: The number of Disconnect and CoA (change of authorization) requests received from the DAC (dynamic authorization client).
- **Authorize Only Requests**: The number of Disconnect and CoA requests received from the DAC with an "Authorize only" Service-Type attribute.
- **Malformed Requests**: The number of malformed Disconnect and CoA requests received from the DAC.
- **Bad Authenticator Requests**: The number of Disconnect and CoA requests received from this DAC with an invalid authenticator field.
- **Dropped Requests**: The number of Disconnect and CoA requests from this DAC that have been silently discarded for reasons other than malformed, bad authenticators, or unknown type.
- **Total ACK Responses**: The number of Disconnect-ACKs sent to the DAC.
- **Total NAK Responses**: The number of Disconnect-NAKs sent to the DAC.
- **Session Not Found Responses**: The number of Disconnect-NAKs sent to the DAC because no session context could be found.
- **User Sessions Modified**: The number of user sessions for which authorization changed due to Disconnect and CoA requests received from the DAC.

Example

Showing RADIUS dynamic authorization statistics for client 1.1.2.1 on VRF default:

```
switch# show radius dyn-authorization client 1.1.2.1 vrf default
Status and Counters - RADIUS Dynamic Authorization Client Information

  VRF Name                 : default
  Authorization Client     : 1.1.2.1
  Unknown Packets          : 55
  Message-Type                    Disconnect       CoA
  ------------------------------------------------------------------
  Total Requests                  2147483647       10
  Authorize Only Requests         10               10
  Malformed Requests              10               10
  Bad Authenticator Requests      2147483647       2147483647
  Dropped Requests                10               10
  Total ACK Responses             10               10
  Total NAK Responses             10               10
  Session Not Found Responses     10               10
  User Sessions Modified          20               20
```

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
6000 6100	Operator (>) or Manager (#)	Operators 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 dyn-authorization client tls (RadSec)

`show radius dyn-authorization client <IP-ADDR> tls [vrf <VRF-NAME>]`

Description

Shows RADIUS dynamic authorization statistics for the specified client (with TLS) on the specified VRF.

Parameter	Description
<IP-ADDR>	Specifies the client IPv4 or IPv6 address.
`vrf` *<VRF-NAME>*	Specifies the VRF on which the identified client is connected. When omitted, VRF **default** is assumed.

Usage

Show command output item identification:

- **Total Requests**: The number of Disconnect and CoA (change of authorization) requests received from the DAC (dynamic authorization client).
- **Authorize Only Requests**: The number of Disconnect and CoA requests received from the DAC with an "Authorize only" Service-Type attribute.
- **Malformed Requests**: The number of malformed Disconnect and CoA requests received from the DAC.
- **Bad Authenticator Requests**: The number of Disconnect and CoA requests received from this DAC with an invalid authenticator field.
- **Dropped Requests**: The number of Disconnect and CoA requests from this DAC that have been silently discarded for reasons other than malformed, bad authenticators, or unknown type.
- **Total ACK Responses**: The number of Disconnect-ACKs sent to the DAC.
- **Total NAK Responses**: The number of Disconnect-NAKs sent to the DAC.
- **Session Not Found Responses**: The number of Disconnect-NAKs sent to the DAC because no session context could be found.
- **User Sessions Modified**: The number of user sessions for which authorization changed due to Disconnect and CoA requests received from the DAC.

Example

Showing RADIUS dynamic authorization statistics for client 1.1.2.1 with TLS enabled on VRF default:

```
switch# show radius dyn-authorization client 1.1.2.1 vrf default
Status and Counters - RADIUS Dynamic Authorization Client Information

  VRF Name                 : default
  Authorization Client     : 1.1.2.1
  TLS Enabled              : Yes
  Unknown Packets          : 55
  Message-Type                    Disconnect       CoA
  ------------------------------------------------------------
  Total Requests                  2147483647       10
  Authorize Only Requests         10               10
  Malformed Requests              10               10
  Bad Authenticator Requests      2147483647       2147483647
  Dropped Requests                10               10
  Total ACK Responses             10               10
  Total NAK Responses             10               10
  Session Not Found Responses     10               10
  User Sessions Modified          20               20
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Chapter 80
Remote AAA (TACACS+, RADIUS) commands

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

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
<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**, **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.
`start-stop`	Selects accounting information capture at both the beginning and 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.

Parameter	Description
	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 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
<CONNECTION-TYPE>	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 <*GROUP-LIST*>, 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 <*GROUP-LIST*>, 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 <GROUP-LIST>`	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
	▪ <*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 32 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 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**

Parameter	Description
	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.

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 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
```

Deleting a RADIUS server with an IPv4 address and specified VRF:

```
switch(config)# no radius-server host 1.1.1.1 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	`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 32 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.

Parameter	Description
	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 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**.

Parameter	Description
[*<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. For *<ENCRYPT-TYPE>* 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 **<ENCRYPT-KEY-TYPE>** is not followed by **<ENCRYPT-KEY>**, plaintext encryption key prompting occurs upon pressing Enter. Enter must be pressed immediately after the **<ENCRYPT-KEY-TYPE>** 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 1abc
```

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 1abc
```

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
10.07 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 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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

radius-server host tls tracking-method

```
radius-server host {<FQDN> | <IPV4> | <IPV6>} tls tracking-method {status-server | keep-alive | access-request}
no radius-server host {<FQDN> | <IPV4> | <IPV6>} tls tracking-method {status-server | keep-alive | access-request}
```

Description

Configures the tracking method to be used for RADIUS server tracking. RADIUS server tracking must be configured for enabling the tracking method. Default tracking method is **access-request**.

The **no** form of this command sets the tracking method to the default option, **access-request**.

Parameter	Description
`{<FQDN> | <IPV4> | <IPv6>}`	Specifies the RADIUS server as: ■ *<FQDN>*: a fully qualified domain name. ■ *<IPV4>*: an IPv4 address. ■ *<IPV6>*: an IPv6 address.
`tracking-method {status-server | keep-alive | access-request}`	Specifies the tracking method for RadSec tracking. Following methods are supported: ■ **status-server:** Status server responses are used to update the reachability status of the RadSec server. ■ **keep-alive:** Server socket status is verified to update the reachability status of the RadSec server. **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. ■ **access-request:** Access response messages are used to update the reachability status of the RadSec server.

Usage

- If the network has a RADIUS proxy, then it is recommended to use the **access-request** tracking method to track the RadSec server.
- If **keep-alive** is the tracking method, then make sure to check whether the server has the capability to treat the **keep-alive** messages sent in RadSec sessions as valid RadSec messages to keep the session active.

Examples

Configuring the RADIUS server tracking method on host **1.1.1.1**:

```
switch(config)# radius-server host 1.1.1.1 tls tracking-method status-server
```

Deleting the RADIUS server tracking method on host **1.1.1.1** and setting the method to the default, **access-request**:

```
switch(config)# no radius-server host 1.1.1.1 tls tracking-method access-request
```

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

Command History

Release	Modification
10.10	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 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 status-server interval

```
radius-server status-server interval <10-86400>
no radius-server status-server interval <10-86400>
```

Description

Configures the time interval in seconds to send the status server requests to the RADIUS server.

The **no** form of this command configures the default time interval, **300** seconds.

Parameter	Description
<10-86400>	Specifies the status server time interval in seconds. Default: **300**.

Examples

Configuring the status server time interval of 200 seconds:

```
switch(config)# radius-server status-server interval 200
```

Resetting the status server time interval to the default, 300 seconds:

```
switch(config)# no radius-server status-server interval 200
```

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
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 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
`interval <INTERVAL>`	Specifies the time interval, in seconds, to wait before checking the server reachability status. Default: 300. Range 60 to 84600.
`retries <RETRIES>`	Specifies the number of server retries. Default: Global RADIUS retries. Range: 0 to 5.

`user-name <NAME>`
`[password [plaintext <PASSWORD> |`
`ciphertext <PASSWORD>]]`
	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.

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)# 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>} [port <PORT-NUMBER>] [vrf <VRF-NAME>]
no server {<FQDN> | <IPV4> | <IPV6>} [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 4100i, 6000, 6100, 6200, 6300, 6400, 8100, 8325, 8360, and 10000 Switch Series, a RADIUS server can be associated with a maximum of four different user-defined server groups.

On the 8320, 8400, and 9300 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.
`port <PORT-NUMBER>`	Specifies the authentication port number. Range: 1 to 65535. Default TACACS+ (TCP): 49, RADIUS (UDP): 1812. 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 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
```

Description

Shows the accounting configuration per connection type (channel).

Examples

Configuring and then showing the accounting sequence for TACACS+ groups and local:

```
(config)# aaa accounting all-mgmt default start-stop group sg1 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 sg1 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
--------------------------------------------------------------------------------
sg1                           | 0
tacacs                        | 1
--------------------------------------------------------------------------------
Accounting for console channel:
--------------------------------------------------------------------------------
GROUP NAME                    | GROUP PRIORITY
--------------------------------------------------------------------------------
local                         | 0
--------------------------------------------------------------------------------
Accounting for default channel:
--------------------------------------------------------------------------------
GROUP NAME                    | GROUP PRIORITY
--------------------------------------------------------------------------------
sg1                           | 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
```

Description

Shows the authentication configuration per connection type (channel).

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
```

Description

Shows the authorization configuration per connection type (channel).

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]
```

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.

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]
```

Description

Shows configured RADIUS servers information.

Parameter	Description
detail	Selects additional RADIUS server details and global parameters for showing.

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
Tracking Time Interval (seconds): 60
Tracking Retries: 5
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1

-----------------------------------------------------------------------
SERVER NAME                                  | PORT | VRF
-----------------------------------------------------------------------
20.1.1.129                                   | 1812 | default
1.1.1.4                                      | 1812 | default
1.1.1.5                                      | 12   | default
abc1.com                                     | 32   | default
2001:0db8:85a3:0000:0000:8a2e:0371:7334      | 1812 | default
-----------------------------------------------------------------------
```

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
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
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
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 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>]  }
```

Description

Shows information for one or all RADIUS servers configured with IPsec.

Parameter	Description
`server-list`	Selects all servers for showing.
`{<FQDN> | <IPV4> | <IPv6>}`	Specifies the RADIUS server as: ■ *<FQDN>*: a fully qualified domain name. ■ *<IPV4>*: an IPv4 address. ■ *<IPV6>*: an IPv6 address.
`port <PORT-NUMBER>`	Specifies the authentication port number. Range: 1 to 65535. Default: 1812.
`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

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 platorms	Operator (>) or Manager (#)	Operators 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]
```

Description

Shows the configured TACACS+ servers.

Parameter	Description
`detail`	Selects additional TACACS+ server details and global parameters for showing.

Examples

Showing a summary of a global TACACS+ configuration with a shared-secret:

```
switch# show tacacs-server
******* Global TACACS+ Configuration *******

Shared-Secret: AQBapb+HsdpqV1Q3CPCBMQTG8e1cA+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+HsdpqV1Q3CPCBMQTG8e1cA+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+HsdpqV1Q3CPCBMQTG8eeA8BEgikCgAAAJOwZSNzA2SWrLA=
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+HsdpqV1Q3CPCBMQTG8eeA8BEgikCgAAAJOwZSNzA2SWrLA=
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+HsdpqV1Q3CPCBMQTG8eeA8BEgikCgAAAJOwZSNzA2SWrLA=
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+AncIRY92hDTYkQCAAAAFEAaHn43vNC
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
```

Description

Shows authentication statistics for all configured TACACS+ servers.

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 accouting 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+HsdpqV1Q3CPCBMQTG8ekK1c...fbeA8BEgikCgAAAJOwZSNzA2SWrLA=
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...9j2AUxlGAAAAF2MkfMTojqX
```

```
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+HsdpqV1Q3CPCBMQTG8ekK1cA+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 32 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
10.07 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 31 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
10.07 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
`interval <INTERVAL>`	Specifies the time interval, in seconds, to wait before checking the server reachability status. Default: 300. Range 60 to 84600.

`user-name <NAME>`
`[password [plaintext <PASSWORD> |`
`ciphertext <PASSWORD>]]`
	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.
	
	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	`config`	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.

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 is reached, the log will display three dots (...) to indicate that the log an 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.

Parameter	Description
`disable`	Disable remote syslog confguration. This does not delete the configuration, just disables/pauses the forwarding of syslog messagesto 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 Seconds
`severity <LEVEL>`	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.
`vrf <VRF-NAME>`	Specifies the VRF used to connect to the syslog server. Optional. Default: `default`

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
	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: ArubaOS-CX format)

The 'no' form of this command will change the accounting log message format to ArubaOS-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 from an earlier version of AOS-CX to AOS-CX 10.11 or later 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 an earlier version to AOS-CX 10.11 or later without configuring this setting, by default, the accounting log message format will be ArubaOS-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 ArubaOS-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.
`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_lldp_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: ■ **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.

Parameter	Description
`severity <LEVEL>`	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
10.07 or earlier	--

Command Information

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

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

show capacities rpvst

```
show capacities rpvst
```

Description

Shows the capacities of RPVST VLANs configurable on a system and RPVST VPORTs supported in a system.

Examples

Showing capacities:

```
switch# show capacities rpvst
System Capacities : Filter RPVST
Capacities Name                                                          Value
------------------------------------------------------------------------------
Maximum number of RPVST VLANs configurable on the system                  32
Maximum number of RPVST VPORTs supported in a system                     512
```

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 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
```

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**.

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 `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 detail

`show spanning-tree detail`

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**.

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

                                          Root Hello Max Fwd
VLAN     Priority Root ID                 cost  Time Age 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>`

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.

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`

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.

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 on the interface. This is the default.

Parameter	Description
<INTERVAL>	Specifies the re-enable timeout in seconds. Range: 1 to 65535.

Example

Enabling the BPDU guard timeout on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# spanning-tree bpdu-guard timeout 10
```

Disabling BPDU guard timeout 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	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).
`rpvst`	Sets the STP mode to RPVST.
`auto-vlan-enable`	Selects RPVST auto VLAN mode.
`priority <NUMBER>`	Specifies the priorites 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.

diagnostic monitor

```
diagnostic monitor {line-module | management-module} [<SLOT-ID>]
no diagnostic monitor {line-module | management-module} [<SLOT-ID>]
```

Description

Enables runtime diagnostics for all modules or for a specified module. This feature is enabled by default for all modules.

The **no** form of this command disables runtime diagnostics for all modules or for a specified module.

Parameter	Description
`line-module`	Specifies the enabling of diagnostic monitoring specific to a line module.
`management-module`	Specifies the enabling of diagnostic monitoring specific to a management module.
<SLOT-ID>	Specifies the slot ID of a module. Format: member/slot.

Usage

When no parameters are used in the command (**diagnostic monitor** or **no diagnostic monitor**), the command applies to all modules. This command impacts the diagnostics that run periodically. It does not affect on-demand diagnostics.

Example

Enabling runtime diagnostics for a specified module:

```
switch(config)# diagnostic monitor management-module 1/1
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

diag on-demand

`diag on-demand {line-module | management-module} [<SLOT-ID>]`

Description

Runs the diagnostic tests for all modules or for a specified module.

Parameter	Description
`[line-module | management-module]`	Selects the options for enabling or disabling run-time diagnostics for a specific module.
`line-module`	Specifies the enabling of diagnostic monitoring specific to a line module.
`management-module`	Specifies the enabling of diagnostic monitoring specific to a management module.
<SLOT-ID>	Specifies the member/slot for management modules (1/1) and line modules (1/1).

Usage

When no parameters are used in the command (**diag on-demand**), the command applies to all modules.

Examples

Running diagnostic tests for all modules on a 6100 switch:

```
switch# diag on-demand
Fetching Test results.  Please wait ...

Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
LineModule           1/1           13     100%
ManagementModule     1/1           13     100%
```

Running diagnostic tests for a specific module on a 6100 switch:

```
switch# diag on-demand management-module 1/1
Performing diagnostic tests.  Please wait ...
Fetching Test results.  Please wait ...

Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
ManagementModule     1/1           13     100%
```

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
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show diagnostic

`show diagnostic {line-module | management-module} [<SLOT-ID>] {brief | detail}`

Description

Displays the diagnostic test results for all modules or for a specified module.

Parameter	Description
`[line-module | management-module]`	Selects the options for enabling or disabling runtime diagnostics for a specific module.
`line-module`	Specifies the enabling of diagnostic monitoring specific to a line module.
`management-module`	Specifies the enabling of diagnostic monitoring specific to a management module.
<SLOT-ID>	Specifies the member/slot for management modules (1/1) and line modules (1/1)

Usage

When no parameters are used in the command (**show diagnostic**), the command applies to all modules.

Example

Showing diagnostic test results in brief format for all modules on a 6100 switch:

```
switch# show diagnostic brief
Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
ManagementModule     1/1            13     100%
LineModule           1/1            13     100%
```

Showing diagnostic test results in brief format for a specified module on a 6100 switch:

```
switch# show diagnostic line-module brief

Module               ID    Diagnostics Success
                           Performed
-------------------- ----- ----------- -------
LineModule           1/1           13     100%
```

Showing diagnostic test results in detail format for all modules on a 6100 switch:

```
switch# show diagnostic detail

Module : ManagementModule 1/1

Diagnostic     Status Error Code History Code Successive    Total Failure Total
  Last Run Timestamp   First Run Timestamp
                                              Failure Count Count
Iteration
-------------- ------ ---------- ------------ ------------- ------------- --------
-  -------------------- --------------------
ddr_cecount    Pass   0x0        0x0                      0             0
109  2019-07-31 16:43:38  2019-07-31 07:44:55
emmc           Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55
fan_ctrlr      Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55
fepld          Pass   0x0        0x0                      0             0
109  2019-07-31 16:43:38  2019-07-31 07:44:54
fru_eeprom     Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:54
fru_eeprom_ul  Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:54
mm_lcb         Pass   0x0        0x0                      0             0
109  2019-07-31 16:43:37  2019-07-31 07:44:54
pmc            Pass   0x0        0x0                      0             0
109  2019-07-31 16:43:37  2019-07-31 07:44:54
rdimm_spd      Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55
rdimm_tmp      Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55
rtc            Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55
tmp1           Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55
tmp2           Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:04  2019-07-31 07:44:55


Module : LineModule 1/1

Diagnostic     Status Error Code History Code Successive    Total Failure Total
  Last Run Timestamp   First Run Timestamp
                                              Failure Count Count
Iteration
-------------- ------ ---------- ------------ ------------- ------------- --------
-  -------------------- --------------------
lc_asic        Pass   0x0        0x0                      0             0
108  2019-07-31 16:43:37  2019-07-31 07:46:03
poe_ctrlr_1_q1 Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:03
poe_ctrlr_1_q2 Pass   0x0        0x0                      0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:04
```

```
poe_ctrlr_1_q3 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:04
poe_ctrlr_2_q1 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:05
poe_ctrlr_2_q2 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:05
poe_ctrlr_2_q3 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:05
poe_ctrlr_3_q1 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:06
poe_ctrlr_3_q2 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:16  2019-07-31 07:46:06
poe_ctrlr_3_q3 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:17  2019-07-31 07:46:06
poe_ctrlr_4_q1 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:17  2019-07-31 07:46:07
poe_ctrlr_4_q2 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:17  2019-07-31 07:46:07
poe_ctrlr_4_q3 Pass    0x0         0x0                    0             0
4  2019-07-31 16:08:17  2019-07-31 07:46:08
```

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
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show diagnostic events

```
show diagnostic events
```

Description

Displays the diagnostic related event logs.

Example

Showing diagnostic related event logs:

```
switch# show diagnostic events
2019-08-07:17:19:21.214532|hhmd|106001|ERR|
Diagnostic mm_mcbe failed with error code 0x380 on management module 1/1
2019-08-07:17:19:21.214554|hhmd|106001|ERR|
```

```
Diagnostic pmc failed with error code 0x4 on management module 1/1
2019-08-07:17:19:21.215532|hhmd|106001|ERR|
Diagnostic ledpld failed with error code 0x4 on management module 1/1
2019-08-07:17:19:21.353221|hhmd|106001|ERR|
Diagnostic mm_mcbe failed with error code 0x380 on management module 1/1
2019-08-07:17:19:21.354421|hhmd|106001|ERR|
Diagnostic pmc failed with error code 0x4 on management module 1/1
2019-08-07:17:19:21.453221|hhmd|106001|ERR|
Diagnostic ledpld failed with error code 0x4 on management module 1/1
```

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
6000 6100	Manager (#)	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 jl726a!Version AOS-CX FL.10.06.0001
module 1/1 product-number jl661a!Version AOS-CX XL.10.00.0002
module 1/1 product-number jl363a!Version AOS-CX PL.10.06.0001
module 1/1 product-number jl677a
!
!
!
!
!
!
```

```
!
vlan 1
interface 1/1/1
    no shutdown
```

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 jl726a!Version AOS-CX FL.10.06.0001
module 1/1 product-number jl661a!Version AOS-CX XL.10.00.0002
module 1/1 product-number jl363a!Version AOS-CX PL.10.06.0001
module 1/1 product-number jl677a
!
!
!
no fastboot
!
!
!
!
vlan 1
interface 1/1/1
    no shutdown
```

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]
show selftest line-module <SLOT-ID>
show selftest line-module <SLOT-ID> interface [brief]
show selftest interface [<PORT-NUM>]
```

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.

Examples

Displaying the output when fastboot is enabled:

```
switch# show selftest
Name       Id   Status         ErrorCode  LastRunTime
---------- ---- -------------- ---------- --------------------
LineModule 1/1  passed         0x0
LineModule 1/2  passed         0x0

switch# show selftest line-module
Name       Id   Status         ErrorCode LastRunTime
---------- ---- -------------- --------- --------------------
LineModule 1/1  passed         0x0
LineModule 1/2  passed         0x0

switch# show selftest line-module 1/1
Name       Id   Status         ErrorCode LastRunTime
---------- ---- -------------- --------- --------------------
LineModule 1/1  passed         0x0
```

Displaying the output when fastboot is enabled:

```
switch# show selftest interface 1/1/2
Name    Status         ErrorCode LastRunTime
------- -------------- --------- --------------------
1/1/2   skipped        0x0

switch# show selftest line-module 1/1 interface
Name    Status         ErrorCode LastRunTime
------- -------------- --------- --------------------
1/1/1   skipped        0x0
1/1/2   skipped        0x0
1/1/3   skipped        0x0
1/1/31  skipped        0x0
```

Displaying the output when fastboot is disabled:

Testing to register read/write:

This test is run irrespective of fastboot being enabled or disabled.

```
switch# show selftest

Name       Id   Status         ErrorCode  LastRunTime
---------- ---- -------------- ---------- -------------------
LineModule 1/1  passed         0x0        2018-02-16 18:15:53
```

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 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 16777215. 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>]`

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.

Examples

Showing sFlow information for all interfaces:

```
switch# show sflow
sFlow Global Configuration
----------------------------------------
sFlow                          enabled
Collector IP/Port/Vrf          10.10.10.2/6343/default
Agent Address                  10.0.0.1
Sampling Rate                  1024
Polling Interval               30
Header Size                    128
Max Datagram Size              1400

sFlow Status
----------------------------------------
Running - Yes

sFlow enabled on Interfaces:
----------------------------------------
lag100

sFlow Statistics
----------------------------------------
Number of Samples              200
```

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
Number of Samples              30
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
Number of 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
10.07 or earlier	--

Command Information

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

Configuration commands

smartlink group

```
smartlink group <GROUP-ID>
no smartlink group <GROUP-ID>
```

Description

Creates a Smartlink group with specified ID.

The **no** form of this command removes the Smartlink group and all associated configurations for a specified ID.

Parameter	Description
<GROUP-ID>	Specifies ID for the Smartlink group.

Usage

The maximum number of Smartlink groups is 24.

Examples

Configuring a Smartlink group:

```
switch(config)# smartlink group 2
switch(config-smartlink-2)#
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

smartlink recv-control-vlan

```
smartlink recv-control-vlan <VID-LIST>
no smartlink recv-control-vlan <VID-LIST>
```

Description

Configures control VLANs to receive flush messages.

The **no** form of this command disables VLANs from receiving flush messages.

Parameter	Description
<VID-LIST>	Specifies VLAN ID.

Usage

- Configure this command on uplink devices where MAC flush is required.
- A flush message clears stale MAC and ARP entries enabling fast traffic convergence.

Examples

Configuring control VLAN to receive flush messages:

```
switch(config)# smartlink recv-control-vlan 2,3
```

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
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

Group context commands

description

```
description <DESC>
no description
```

Description

Adds description to a Smartlink group.

The **no** form of this command removes a description from a Smartlink group.

Parameter	Description
<DESC>	Specifies description for a Smartlink group. 1 to 64 printable ASCII characters are allowed.

Examples

Adding a description to a Smartlink group:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# Description for group 3
```

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
6000 6100	config-smartlink-*<GROUP>*	Administrators or local user group members with execution rights for this command.

diag-dump smartlink basic

```
diag-dump smartlink basic
```

Description

Dumps the Smartlink configuration, state and statistics.

Examples

Dump of Smartlink configuration, state, and statistics:

```
switch# diag-dump smartlink basic
================================================================================
[Start] Feature smartlink Time : Tue Jul  7 10:08:31 2020
================================================================================
--------------------------------------------------------------------------------
[Start] Daemon smartlinkd
--------------------------------------------------------------------------------
SL Group 1: Primary port 1/1/1 Secondary port 1/1/2 Control VLAN 4,
            Preemption disabled, Preemption-delay 1 Preemption Timer OFF,
            State primary_with_backup, Active port PRIMARY, Backup port SECONDARY
Port 1/1/1: member_groups 1 SL Groups ids: 1, 0
```

```
Port 1/1/2: member_groups 1 SL Groups ids: 1, 0

or

SL Group 1: Primary port lag1    (mclag: local_up_remote_up)
            Secondary port lag2 (mclag: local_down_remote_up), Control VLAN 4,
            Preemption disabled, Preemption-delay 1 Preemption Timer OFF,
            State primary_with_backup, Active port PRIMARY, Backup port SECONDARY
Port lag1: member_groups 1 SL Groups ids: 1, 0
Port lag2: member_groups 1 SL Groups ids: 1, 0
VSX Oper Status: Primary/Secondary/NA

------------------------------------------------------------------------------
[End] Daemon smartlinkd
------------------------------------------------------------------------------
------------------------------------------------------------------------------
[Start] Daemon ops-switchd
------------------------------------------------------------------------------
Group-ID | Port Name | Port Status | Vlan-ID | HW-Port-State | Vlan-Type
1        | 1/1/1     | Active      | 4       | Forwarding    | Control
1        | 1/1/1     | Active      | 3       | Forwarding    | Protected
1        | 1/1/1     | Active      | 2       | Forwarding    | Protected
1        | 1/1/1     | Active      | 1       | Forwarding    | Protected
1        | 1/1/2     | Backup      | 4       | Blocking      | Control
1        | 1/1/2     | Backup      | 3       | Blocking      | Protected
1        | 1/1/2     | Backup      | 2       | Blocking      | Protected
1        | 1/1/2     | Backup      | 1       | Blocking      | Protected

------------------------------------------------------------------------------
[End] Daemon ops-switchd
------------------------------------------------------------------------------
==============================================================================
[End] Feature smartlink
==============================================================================
Diagnostic-dump captured for feature smartlink
```

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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

primary-port

```
primary-port <INTERFACE-NAME>
no primary-port
```

Description

Configures primary port for a Smartlink group.

The **no** form of this command removes primary port from a Smartlink group.

Parameter	Description
<INTERFACE-NAME>	Specifies interface for primary port.

Examples

Configuring primary port for a Smartlink group:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# primary-port 1/1/1
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	config-smartlink-*<GROUP>*	Administrators or local user group members with execution rights for this command.

smartlink group secondary-port

```
secondary-port <INTERFACE-NAME>
no secondary-port
```

Description

Configures secondary port for a Smartlink group.

The **no** form of this command removes secondary port from a Smartlink group.

Parameter	Description
<INTERFACE-NAME>	Specifies interface for secondary port.

Examples

Configuring secondary port for a Smartlink group:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# secondary-port 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
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	config-smartlink-*<GROUP>*	Administrators or local user group members with execution rights for this command.

control-vlan

```
control-vlan <VLAN-ID>
no control-vlan <VLAN-ID>
```

Description

Configures control VLAN in a Smartlink group.

The **no** form of this command removes control VLAN from a Smartlink group.

Parameter	Description
<VLAN-ID>	Specifies VLAN ID for a Smartlink group.

Usage

- In a Smartlink group, the control VLAN is used to send flush messages.
- Control VLAN is configured on the device intended to send flush messages.
- Each Smartlink group must use a unique control VLAN.
- Control VLAN is protected in the Smartlink group to avoid loops.

Examples

Configuring control VLAN in a Smartlink group:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# control-vlan 10
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	`config-smartlink-<GROUP>`	Administrators or local user group members with execution rights for this command.

protected-vlans

```
protected-vlans <VLAN-ID-LIST>
no protected-vlans <VLAN-ID-LIST>
```

Description

Specifies VLANs protected by a Smartlink group.

The **no** form of this command removes VLANs protected by a Smartlink group.

Parameter	Description
<VLAN-ID-LIST>	Specifies list of VLAN IDs. Range is 1 to 4094.

Examples

Configuring protected VLANs for a Smartlink group.:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# protected-vlans 1, 10-50
```

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
6000 6100	`config-smartlink-<GROUP>`	Administrators or local user group members with execution rights for this command.

preemption

```
preemption
no preemption
```

Description

Configures preemption in a Smartlink group.

The **no** form of this command disables preemption in a Smartlink group.

Usage

- If preemption is enabled, a recovered primary port preempts the active interface after the configured preemption delay.
- If preemption is disabled, a recovered primary port serves as a backup interface and does not forward traffic.

Examples

Configuring preemption in a Smartlink group:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# preemption
```

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
6000 6100	`config-smartlink-<GROUP>`	Administrators or local user group members with execution rights for this command.

preemption-delay

```
preemption-delay <SECONDS>
no preemption-delay
```

Description

Specifies preemption delay for a Smartlink group.

The **no** form of this command removes previously configured preemption delay from a Smartlink group and sets it to the default of 1 second.

Parameter	Description
<SECONDS>	Specifies preemption delay in seconds. Range is 0 to 300 seconds.

Usage

When preemption is enabled, a recovered primary port always preempts the active interface after the configured preemption delay.

Examples

Configuring preemption delay on a Smartlink group:

```
switch(config)# smartlink group 3
switch(config-smartlink-3)# preemption
switch(config-smartlink-3)# preemption-delay 10
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	config-smartlink-*<GROUP>*	Administrators or local user group members with execution rights for this command.

Display commands

show smartlink group

```
show smartlink group <GROUP-ID>
```

Description

Shows information for a specific Smartlink group.

Parameter	Description
<GROUP-ID>	Specifies Smartlink group ID.

Examples

Showing Smartlink group information:

```
switch# show smartlink group 1
Smartlink Group 1 Information:
==============================
Group description          : Uplink1
Protected VLANs            : 20-30
Control VLAN               : 10
Preemption                 : ON
Preemption Delay           : 10
Ports  Role      State      Flush Count Last Flush Time
------ --------- ---------- ----------- -------------------------
1/1/1  Primary   Active     2           Sat Oct 17 19:09:10 2020
1/1/2  Secondary Backup     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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show smartlink group all

```
show smartlink group all
```

Description

Shows information for all configured Smartlink groups.

Examples

Showing information for all configured Smartlink groups:

```
switch# show smartlink group all
Smartlink Group Information:
============================
     Primary Secondary  Active  Backup   Ctrl      Preemption Preemption
Grp  Port    Port       Port    Port     Vlan                 Delay
---- ------- ---------  ------  -------  --------- ---------- ----------
1    1/1/1   1/1/2      1/1/1   1/1/2    10          OFF        1
2    1/1/5   1/1/6      1/1/5   1/1/6    11          OFF        1
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show smartlink group detail

```
show smartlink group detail
```

Description

Shows detailed information for all configured Smartlink groups.

Examples

Showing detailed information for all configured Smartlink groups:

```
switch# show smartlink group detail
Smartlink Group 1 Information:
==============================
Protected VLAN                : 1-3
Control VLAN                  : 1
Preemption                    : OFF
Preemption Delay              : 1
Ports    Role         State        Flush Count  Last Flush Time
-------- ------------ ------------ ------------ ------------------------
1/3/1    Primary      Backup       0
1/3/2    Secondary    Active       0

Smartlink Group 2 Information:
==============================
Protected VLAN                : 4-6
Control VLAN                  : 4
Preemption                    : OFF
Preemption Delay              : 1
Ports    Role         State        Flush Count  Last Flush Time
-------- ------------ ------------ ------------ ------------------------
1/3/2    Primary      Active       0
1/3/1    Secondary    Backup       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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show smartlink flush-statistics

```
show smartlink flush-statistics
```

Description

Shows information for received flush messages.

Usage

This command must be executed on an uplink or peer device configured with **recv-control-vlan**.

Examples

Showing information for received flush messages:

```
switch# show smartlink flush-statistics
Last Flush Packet Detail:
=========================

Flush Packets Received                       : 2
Last Flush Packet Received On Interface      : 1/1/1
Last Flush Packet Received On                : Sat Oct 17 19:09:10 2020
Device Id Of Last Flush Packet Received      : 5065f3-127080
Control VLAN Of Last Flush Packet Received   : 10
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	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 smartlink group statistics

```
clear smartlink group [<GROUP-ID>] statistics
```

Description

Clears Smartlink statistics for the specified Smartlink group or all Smartlink groups.

Parameter	Description
<GROUP-ID>	Specifies Smartlink group.

Examples

Clearing Smartlink statistics for a specified Smartlink group:

```
switch# clear smartlink group 1 statistics
```

Clearing all Smartlink statistics for all Smartlink groups:

```
switch(config)# clear smartlink group statistics
```

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
6000 6100	Operator (>) or Manager (#)	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 smartlink flush-statistics

```
clear smartlink flush-statistics
```

Description

Clears Smartlink flush statistics.

Usage

This command must be executed on the uplink device configured with **recv-control-vlan**.

Examples

Clearing Smartlink flush statistics:

```
switch# clear smartlink flush-statistics
```

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
6000 6100	Operator (>) or Manager (#)	Operators 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

Shows current running configuration.

Examples

Showing currently running configuration:

```
switch# configure terminal
switch(config)# smartlink group 1
switch(config-smartlink-1)# description Uplink1
switch(config-smartlink-1)# primary-port 1/1/1
switch(config-smartlink-1)# secondary-port 1/1/2
switch(config-smartlink-1)# control-vlan 10
switch(config-smartlink-1)# protected-vlans 20-30
switch(config-smartlink-1)# preemption
switch(config-smartlink-1)# preemption-delay 10
switch(config)# smartlink group 2
switch(config-smartlink-2)# primary-port 1/1/8
switch(config-smartlink-2)# secondary-port 1/1/9
switch(config-smartlink-2)# control-vlan 11
switch(config-smartlink-2)# protected-vlans 20-30
switch# show running-config
Current configuration:
```

```
!
!
!
smart-link group 1
  primary-port 1/1/1
  secondary-port 1/1/2
  control-vlan 10
  protected-vlans 20-30
  preemption
  preemption-delay 10
  exit
smart-link group 2
  primary-port 1/1/8
  secondary-port 1/1/9
  control-vlan 11
  protected-vlans 20-30
  exit
```

For more information on features that use this command, refer to the Link Aggregation Guide for your switch model.

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Supportability commands

show capacities smartlink

```
show capacities smartlink | show capacities-status smartlink
```

Description

Shows Smartlink capacities or Smartlink capacities and status.

Examples

Showing Smartlink capacities:

```
switch# show capacities smartlink

System Capacities: Filter SMARTLINK
Capacities Name
```

```
Value
------------------------------------------------------------------------------
--
Maximum number of SMARTLINK GROUPS configurable in a system
24
```

Showing Smartlink capacities and status:

```
switch# show capacities-status smartlink

System Capacities Status: Filter SMARTLINK
Capacities Status Name                                                  Value
Maximum
------------------------------------------------------------------------------
--
Number of SMARTLINK GROUPS currently configured                           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
6000 6100	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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	`config` and `config-if`	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
`aged`	Notifies when a MAC address aged out on the interface.
`learned`	Notifies when a MAC address is learned on the interface.
`moved`	Notifies when a MAC address moved from the interface.
`removed`	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 *View* column is added to the command output.
10.08	Added *ACL Type* 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
```

```
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   ro            view1
                                         context1
                                         context3
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 *View* 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
```

The `deny` rule is not supported for SNMP 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
`interface <IF-NAME>`	Specifies the source interface name. The interface can be a physical interface, loopback interface, or VLAN interface.
<IPv4-ADDRESS>	Specifies the IPv4 address of the source interface for the SNMP response.
<IPv6-ADDRESS>	Specifies the IPv6 address of the source interface for the SNMP response.
`vrf <VRF-NAME>`	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	`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.

Parameter	Description
<IPv4-ADDR>	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**.
<IPv6-ADDR>	Specifies the IP address of a trap receiver in IPv6 format (**x:x::x:x**).
`trap version` *<VERSION>*	Specifies the trap notification type for SNMPv1, v2c or v3. Available options are: **v1**, **v2c** or **v3**.

Parameter	Description
`inform version v2c`	Specifies the inform notification type for SNMPv2c.
`trap version v3`	Specifies the trap notification type for SNMPv3.
`user <NAME>`	Specifies the SNMPv3 user name to be used in the SNMP trap notifications.
`community <STRING>`	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**.
<UDP-PORT>	Specifies the UDP port on which notifications are sent. Range: 1 - 65535. Default: 162.
<VRF-NAME>	Specifies the VRF on which the SNMP agent listens for incoming requests.
<notification-type>	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 ■ 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
<DESCRIPTION>	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
<INFO>	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 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

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 port-security

```
snmp-server trap port-security
no snmp-server trap port-security
```

Description

Enables SNMP port-security violation traps on the system. Port-security violation traps are enabled by default.

The **no** form of this command disables the SNMP port-security violation traps on the system.

Parameter	Description
`port-security`	Specifies SNMP traps for port-security.

Examples

Enabling the SNMP port-security violation traps on the system:

```
switch(config)# snmp-server trap port-security
```

Disabling the SNMP port-security violation traps on the system:

```
switch(config)# no snmp-server trap port-security
```

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
6000 6100	`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.

Parameter	Description
<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**.

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 (?).
`vrf` *<VRF-NAME>*	Specifies the VRF associated with the context. Default: default.
`community` *<STRING>*	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	`config`	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	`config`	Administrators or local user group members with execution rights for this command.

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 Aruba 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`

Parameter	Description
	Selects TFTP.
	Specifies the VRF name.
<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 1/1/1configuration 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 protocl on VRF green :

```
switch(config)# ip source-interface dns 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1configuration 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 `cental`, `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

`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.

Parameter	Description

	`all`
	Selects all protocols supported by this command.
	`central`
	Selects Aruba Central.
	`dhcp_relay`
	Selects DHCP relay.
	`dns`
	Selects DNS packets
	`http`
	Selects HTTP.
	`ntp`
	Selects NTP.
	`radius`
	Selects radius.
	`sftp-scp`
	Selects SFTP and SCP.
	`sflow`
	Selects sFLow.
	`ssh-client`
	Selects SSH Client.
	`syslog`
	Selects syslog.
	`tacacs`
	Selects TACACS.
	`tftp`
	SelectsTFTP.

<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

<PROTOCOL>	Specifies the protocol to configure.
	`all`
	Selects all protocols supported by this command.
	`central`
	Selects Aruba Central.
	`dhcp_relay`
	Selects DHCP relay.
	`dns`
	Selects DNS packet source.
	`http`
	Selects HTTP.
	`ntp`
	Selects NTP.
	`radius`
	Selects radius.
	`sftp-scp`
	Selects SFTP and SCP.
	`sflow`
	Selects sFLow.
	`ssh-client`
	Selects SSH Client.
	`syslog`
	Selects syslog.
	`tacacs`
	Selects TACACS.
	`tftp`
	SelectsTFTP.
	`ubt`
	SelectsUBT.

<IPV6-ADDR>	Specifies the IPv6 address.
`vrf` *<VRF-NAME>*	Specifies the VRF name.

Examples

Configuring IPv6 source-interface dns :

```
switch(config)# ipv6 source-interface
        all          All protocols
        central      Aruba Central protocol
        dhcp_relay   DHCP_RELAY protocol
        dns          DNS protocol
        http         HTTP protocol
        ntp          NTP protocol
        radius       RADIUS protocol
        sflow        sFlow protocol
        sftp-scp     SFTP and SCP protocols
        ssh-client   SSH Client protocol
```

```
        syslog      syslog protocol
        tacacs      TACACS protocol
        tftp        TFTP protocol
```

Configuring IPv6 source -interface dns:

```
switch(config)# ipv6 source-interface dns
X:X::X:X   Specify an IPv6 address
interface  Interface information
```

Configuring IPv6 source-interface dns on 1: :1:

```
switch(config)# ipv6 source-interface dns 1::1
vrf   VRF Configuration
<cr>
```

Configuring IPv6 source-interface dns on 1: :1: vrf:

```
switch(config)#  ipv6 source-interface dns 1::1 vrf
VRF_NAME  VRF name
```

Configuring IPv6 source-interface dns on 1: :1 vrf BLUE

```
switch(config)# ipv6 source-interface dns 1::1 vrf BLUE
switch(config)# ipv6 source-interface dns interface vlan10
vrf   VRF Configuration
<cr>
```

Configuring IPv6 source-interface dns on vlan10 vrf BLUE:

```
switch(config)# ipv6 source-interface dns interface vlan10 vrf BLUE
```

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

<PROTOCOL>	Specifies the protocol to show.
	`all`
	Shows the source interface configuration for all other protocols.
	`central`
	Shows the source interface configuration for Aruba Central.
	`dhcp relay`
	Shows the source interface configuration for DHCP relay.
	`dns`
	Shows the source interface configuration for DNS.
	`http`
	Shows the source interface configuration for HTTP.
	`ntp`
	Shows the source interface configuration for NTP.
	`radius`
	Shows the source interface configuration for radius.
	`sflow`
	Shows the source interface configuration for sFLow.
	`sftp-scp`
	Shows source interface configuration for SFTP and SCP.
	`ssh-client`
	Shows source interface configuration for SSH Client.
	`syslog`
	Shows the source interface configuration for syslog.
	`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 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 `central`, `sftp-scp`, and `ssh-client` 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

<PROTOCOL>	Specifies the protocol to show.
	`all`
	Shows the source interface configuration for all other protocols.
	`central`
	Shows the source interface configuration for Aruba Central.
	`dhcp_relay`
	Shows the source interface configuration for DHCP realy.
	`dns`
	Shows the source interface configuration for DNS.
	`http`
	Shows the source interface configuration for HTTP.
	`ntp`
	Shows the source interface configuration for NTP.
	`radius`
	Shows the source interface configuration for radius.
	`sflow`
	Shows the source interface configuration for sFLow.
	`sftp-scp`
	Shows source interface configuration for SFTP and SCP.
	`ssh-client`
	Shows source interface configuration for SSH Client.
	`syslog`
	Shows the source interface configuration for syslog.
	`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 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
```

Displaying all IPv6 source-interface protocol confirgurations 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
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 `dns` parameters.
10.12.1000	Added `central`, `sftp-scp`, and `ssh-client` 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):

Aruba 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 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 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 dns 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 green
     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

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

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 `default` 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.

Chapter 90
SSH client commands

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

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 `default` 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.

On the 6000 and 6100 Switch Series, only the vrf named **default** is available. Replace any references to the **mgmt** or other VRFs with **default**.

show ssh host-key

```
show ssh host-key [ecdsa | ed25519 | rsa]
```

Description

Shows the public host keys for the SSH server. If the key type is not provided, all available host-keys are shown.

Parameter	Description
`ecdsa`	Selects the ECDSA host-key pair.
`ed25519`	Selects the ED25519 host-key pair.
`rsa`	Selects the RSA host-key pair.

Examples

Showing the ECDSA public host-key:

```
switch# show ssh host-key ecdsa

Key Type : ECDSA     Curve : ecdsa-sha2-nistp256

ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAhtuv5rABBBGs
...
O4mjVFGMVKZ87RWkyrxeQa2fAGZZEp1902K33/k3q17fA4EivRzC75YvjDu8=
```

Showing all public host keys:

```
switch# show ssh host-key
Key Type : ECDSA     Curve : ecdsa-sha2-nistp256
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAhtuv5rABBBGs
...
O4mjVFGMVKZ87RWkyrxeQa2fAGZZEp1902K33/k3q17fA4EivRzC75YvjDu8=

Key Type : ED25519
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGb6910Jwoe8Hkl9K5YhqijrWI3yovNbiJVq6tw4WjJr4

Key Type : RSA       Key Size : 2048
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdVCXlw43h4n1bwg9jI6DSBMngymCdPD0JUG42Sn9IS
```

```
...
nGSXtrNy6OmlFDJTAy+zz5Kd8d21ZLuhf07IHNgF3pff65Xc8qNJBv
```

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 ssh server

```
show ssh server [vrf default]
```

Description

Shows the SSH server configuration for the default VRF.

Parameter	Description
`vrf default`	Specifies the default VRF.

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)  : 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-sha2-512ssh-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
```

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 default]
```

Description

Shows the active SSH sessions on the default VRF.

Parameter	Description
`vrf default`	Specifies the default VRF.

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
```

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.

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**

Parameter	Description
	▪ **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** ▪ **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.
`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
<HOST-KEY-ALGORITHMS-LIST>	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	`config`	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
<KEY-EXCHANGE-ALGORITHMS-LIST>	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**

Parameter	Description
	▪ **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.

Parameter	Description
<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**

Parameter	Description
	▪ **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

Parameter	Description
	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
ip <ipv4-addr>[mask]	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
ipv6 <iv6p-addr>[mask]	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 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
<PORT-NUMBER>	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
`vrf <VRF-NAME>`	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	`config`	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> | reject |
   nullroute}
no ip route <DEST-IPV4-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> | reject
|
   nullroute}
```

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.
<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.

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
```

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
All platforms	`config`	Administrators or local user group members with execution rights for this command.

ip route distance

```
ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>] distance <VALUE>
no ip route <DEST-IPV4-ADDR>/<NETMASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>] distance <VALUE>
```

Description

Configures the administrative distance for the IPv4 static route.

The **no** form of this command deletes the static route.

Parameter	Description
<DEST-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.
<NEXT-HOP-IP-ADDR>	Specifies the next hop IPv4 address 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.
`distance` *<VALUE>*	Specifies the administrative distance to associate with this static route. Default: 1. Range: 1-255.

Examples

```
switch(config)# ip route 10.0.2.0/24 20.0.0.2 distance 4
switch(config)# ip route 10.0.3.0/24 1/1/1 distance 6
```

```
switch(config)# no ip route 10.0.3.0/24 1/1/1 distance 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
6000 6100	config	Administrators or local user group members with execution rights for this command.

ip route tag

```
ip route <DEST-IPV4-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> | reject |
   nullroute} [tag] <1-4294967295>
no ip route <DEST-IPV4-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> | reject
|
   nullroute} [tag] <1-4294967295>
```

Description

Configures tag for IPv4 static route.

The **no** form of this command deletes tag for IPv4 static route.

Parameter	Description
<DEST-IPV4-ADDR>/<NETMASK>	Specifies the IPv4 route destination.
<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.
reject	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
nullroute	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.
tag	Specifies and assigns tag for the route.

Examples

```
switch(config)# ip route 10.1.1.1/32 20.1.1.2 tag 10
switch(config)# ip route 10.1.1.5/32 1/1/1 tag 20
```

```
switch(config)# no ip route 10.1.1.1/32 20.1.1.2 tag 10
switch(config)# no route 10.1.1.5/32 1/1/1 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
10.10	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.

ipv6 route

```
ipv6 route <DEST-IPV6-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> | reject
|   nullroute}
no ipv6 route <DEST-IPV6-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> |
   reject | nullroute}
```

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.
<NEXTHOP-PORT-LAG-VLAN>	Specifies the next hop as an outgoing interface.
`reject`	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
`nullroute`	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.

Examples

```
switch(config)# ipv6 route 120::/124 nullroute
switch(config)# ipv6 route 121::/124 nullroute
switch(config)# ipv6 route 122::/124 1/1/1
switch(config)# ipv6 route 122::/124 1/1/1.110
```

```
switch(config)# no ipv6 route 122::/124 1/1/1.110
```

For more information on features that use this command, refer to the IP Routing Guide for your switch model.

Command History

Release	Modification
10.10	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.

ipv6 route distance

```
ipv6 route <DEST-IPV6-ADDR>/<MASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>] distance <VALUE>
no ipv6 route <DEST-IPV6-ADDR>/<MASK> [<NEXT-HOP-IP-ADDR>|<INTERFACE>] distance <VALUE>
```

Description

Configures the administrative distance for the IPv6 static route

The **no** form of this command deletes the static route.

Parameter	Description
<DEST-IPV6-ADDR>	Specifies the route destination 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.
<NEXT-HOP-IP-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.
<INTERFACE>	Specifies the next hop as an outgoing interface.
distance *<VALUE>*	Specifies the administrative distance to associate with this static route. Range: 1 to 255. Default: 1.

Examples

```
switch(config)# ipv6 route 122::/124 1/1/1 distance 5
switch(config)# ipv6 route 123::/124 120::1 distance 6
```

```
switch(config)# no ipv6 route 123::/124 120::1 distance 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
All platforms	`config`	Administrators or local user group members with execution rights for this command.

ipv6 route tag

```
ipv6 route <DEST-IPV6-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> | reject
|
   nullroute} [tag] <1-4294967295>
no ipv6 route <DEST-IPV6-ADDR>/<NETMASK> {<NEXTHOP-ADDR> | <NEXTHOP-PORT-LAG-VLAN> |
   reject | nullroute} [tag] <1-4294967295>
```

Description

Configures tag for IPv6 static route.

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.
<NEXTHOP-PORT-LAG-VLAN>	Specifies the next hop as an outgoing interface.
`reject`	Specifies that packets matching the destination route are discarded and an ICMP error notification is sent to the sender.
`nullroute`	Specifies that packets matching the destination route are silently discarded and no ICMP error notification is sent to the sender.
`tag`	Specifies and assigns tag for the route.

Examples

```
switch(config)# ipv6 route 3001::1/128 1/1/1 tag 10
switch(config)# ipv6 route 3002::1/128 1000::2 tag 20
```

```
switch(config)# no ipv6 route 3001::1/128 1/1/1 tag 10
switch(config)# no ipv6 route 3002::1/128 1000::2 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
10.10	Inclusive language update.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6000 6100	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.
- **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 8325, 10000, 8360, and 9300 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)        :  -
Nexthop         :  -                    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
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
10.07 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

`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.
- **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 8325, 10000, 8360, and 9300 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
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
10.10	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.

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. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ■ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ■ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***

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, or USB.

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: **show accounting log** **show events**
{*<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. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
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 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 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, or USB.

Parameter	Description
<FEATURE>	The name of a feature, for example **aaa or vrrp**. 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: Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*} [:*<PORT>*]/*<FILE>***
vrf *<VRF-NAME>*	Specifies the VRF name. If no VRF name is provided, the VRF named *default* is used. Optional.
<STORAGE-URL>	Specifies the USB to copy command output. Required. 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
```

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, or USB.

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. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*} [:*<PORT>*]/*<FILE>***
`vrf <VRF-NAME>`	Specifies the VRF name. The default VRF name is default. Optional.

Parameter	Description
<STORAGE-URL>	Specifies the USB to copy command output. 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. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
<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. Syntax: **{usb}:/<*FILE*>**
<*REMOTE-URL*>	Specifies the URL to copy the command output. Syntax: ▪ {tftp://}{<*IP*> | <*HOST*>}[:<*PORT*>] [;blocksize=<*VAL*>]/<*FILE*> ▪ **{sftp:// | scp:// <*USER*>@}{<*IP*> | <*HOST*>}[:<*PORT*>]/<*FILE*>**
config <*CONFIG-NAME*>	Specifies the running configuration.
vrf <*VRF-NAME*>	Specifies the VRF name. The default VRF name is default. Optional.

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
10.08	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, and USB.

Parameter	Description
`{<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 URL to copy the command output. Required. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
`vrf <VRF-NAME>`	Specifies the VRF name. The default VRF name is default. Optional.
`<STORAGE-URL>`	Specifies the USB to copy command output. Required. Syntax: **{usb}:/*<FILE>***

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
{<*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 URL to copy the command output. Syntax: ▪ **{tftp://}{<*IP*> | <*HOST*>}[:<*PORT*>] [;blocksize=<*VAL*>]/<*FILE*>** ▪ **{sftp:// | scp:// <*USER*>@}{<*IP*> | <*HOST*>}[:<*PORT*>]/<*FILE*>**
vrf <*VRF-NAME*>	Specifies the VRF name. The default VRF name is default. Optional.
<*STORAGE-URL*>	Specifies the USB to copy command output. Syntax: **{usb}:/<*FILE*>**

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. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*][;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* | *<HOST>*}[:*<PORT>*]/*<FILE>***
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 or USB.

Parameter	Description
<FEATURE-NAME>	The feature name, for example, `aaa`.
{*<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 URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*] [;blocksize=*<VAL>*]/*<FILE>*** ▪ **{sftp:// | scp:// *<USER>*@}{*<IP>* |**

Parameter	Description
	<HOST>*}[:*<PORT>*]/*<FILE>
`vrf <VRF-NAME>`	Specifies the VRF name. The default VRF name is default. Optional.
<STORAGE-URL>	Specifies the USB to copy command output. Syntax: **{usb}:/*<FILE>***

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
```

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, or USB.

You can store only one copy of the support file locally. When you store a new support file, it overwrites the existing support file.

Parameter	Description
<FEATURE-NAME>	Specifies the feature for the support files.
<SLOT-ID>	Specifies the module slot number identifier for the support files. 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
```

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, or USB.

Parameter	Description
<DAEMON-NAME>	Specifies the name of the daemon. Required.
{*<STORAGE-URL>* | *<REMOTE-URL>* [vrf *<VRF-NAME>*]}	Selects 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. Syntax: **{usb}:/*<FILE>***
<REMOTE-URL>	Specifies the URL to copy the command output. Syntax: ▪ **{tftp://}{*<IP>* | *<HOST>*}[:*<PORT>*]**

Parameter	Description
	[;blocksize=<*VAL*>]/<*FILE*> ▪ **{sftp:// | scp:// <*USER*>@}{<*IP*> | <*HOST*>}[:<*PORT*>]/<*FILE*>**
`vrf <VRF-NAME>`	Specifies the VRF name. If no VRF name is provided, the VRF named *default* 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.

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.

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.

front-panel-security factory-reset

```
front-panel-security factory-reset
no front-panel-security factory-reset
```

Description

Enable the **front-panel factory-reset** feature to allow a factory reset via the reset button on the front panel of the switch, without console access. Once the feature is enabled, this setting will be saved across reboots, until a factory-reset is performed. The **no** form of this command disables the front-panel factory-reset feature after it has been enabled. This feature is disabled by default.

Usage

If you enable front-panel factory-reset feature:

- pressing the reset button and releasing it before 5 seconds will reboot the system.
- pressing the reset button and releasing it between 5 to 20 seconds will start a hard reset of the system
- pressing the reset button and releasing it between 20 to 25 seconds will start a hard reset of the system, and the system will undergo the factory reset process.
- pressing the reset button for more than 25 seconds will not trigger any action.

If the front-panel factory-reset feature is left at its default disabled setting in the running configuration :

- pressing the reset button and releasing it before 5 seconds will reboot the system.
- pressing the reset button and releasing it between 5 to 20 seconds mark will start a hard reset of the system.
- pressing the reset button for more than 20 seconds will not trigger any action.

For more information about the LED indicators on this switch, refer to the Installation Guide for your switch.

Example

```
switch(config)# front-panel-security factory-reset
This command will enable front-panel factory reset capability, where user can
trigger factory-reset via reset button. This feature will remain enabled until
it is disabled, or a factory-reset is performed.

Continue (y/n)?
```

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 introduced

Command Information

Platforms	Command context	Authority
6000 6100	`config`	Administrators or local user group members with execution rights for this command.

front-panel-security factory-reset

```
front-panel-security factory-reset
no front-panel-security factory-reset
```

Description

Enable the **front-panel factory-reset** feature to allow a factory reset via the reset button on the front panel of the switch, without console access. Once the feature is enabled, this setting will be saved across reboots, until a factory-reset is performed. The **no** form of this command disables the front-panel factory-reset feature after it has been enabled. This feature is disabled by default.

Usage

If you enable front-panel factory-reset feature:

- pressing the reset button and releasing it before 5 seconds will reboot the system.
- pressing the reset button and releasing it between 5 to 20 seconds will start a hard reset of the system
- pressing the reset button and releasing it between 20 to 25 seconds will start a hard reset of the system, and the system will undergo the factory reset process.
- pressing the reset button for more than 25 seconds will not trigger any action.

If the front-panel factory-reset feature is left at its default disabled setting in the running configuration :

- pressing the reset button and releasing it before 5 seconds will reboot the system.
- pressing the reset button and releasing it between 5 to 20 seconds mark will start a hard reset of the system.
- pressing the reset button for more than 20 seconds will not trigger any action.

For more information about the LED indicators on this switch, refer to the Installation Guide for your switch.

Example

```
switch(config)# front-panel-security factory-reset
This command will enable front-panel factory reset capability, where user can
trigger factory-reset via reset button. This feature will remain enabled until
it is disabled, or a factory-reset is performed.

Continue (y/n)?
```

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 introduced

Command Information

Platforms	Command context	Authority
6000 6100	`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 sets the host name to the default value, which is `switch`.

Parameter	Description
<HOSTNAME>	Specifies the host name. The first character of the host name must be a letter or a number. Length: 1 to 32 characters. Default: `switch`

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)#
```

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 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.

Parameter	Description
`Boot ID`	A unique ID for the boot . A system-generated 128-bit string.
`Current Boot, up for <time>`	For the current boot, the **show boot-history** command shows the number of seconds the module has been running on the current software.
`<Timestamp>: boot reason`	For previous boot operations, the **show boot-history** 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: ■ ***<DAEMON-NAME>* crash**: The daemon identified by *<DAEMON-NAME>* caused the module to boot. ■ **Kernel crash**: The operating system software associated with the module caused the module to boot. ■ **Uncontrolled reboot**: The reason for the reboot is not known. ■ **Reboot requested through database**: The reboot occurred because of a request made through the CLI or other API.

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
```

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>
```

Description

Shows system capacities and their values for all features or a specific feature.

Parameter	Description
<FEATURE>	Specifies a feature. For example, **aaa**.

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 classifier-related capacities on the 6100:

```
switch# show capacities classifier

System Capacities: Filter Classifier
Capacities Name                                                                  Value
--------------------------------------------------------------------------------
--
Maximum number of Access Control Entries configurable in a system
4096
Maximum number of Access Control Lists configurable in a system
512
Maximum number of class entries configurable in a system
4096
Maximum number of classes configurable in a system
512
Maximum number of entries in an Access Control List
1024
```

```
Maximum number of entries in a class
1024
Maximum number of entries in a policy
64
Maximum number of classifier policies configurable in a system
512
Maximum number of policy entries configurable in a system
4096
```

Showing all available capacities on the 6100:

```
switch# show capacities

System Capacities:
Capacities Name
Value
-------------------------------------------------------------------------------
--------
Maximum number of Access Control Entries configurable in a system
 4096
Maximum number of Access Control Lists configurable in a system
  512
Maximum number of class entries configurable in a system
 4096
Maximum number of classes configurable in a system
  512
Maximum number of entries in an Access Control List
 1024
Maximum number of entries in a class
 1024
Maximum number of entries in a policy
   64
Maximum number of classifier policies configurable in a system
  512
Maximum number of policy entries configurable in a system
 4096
Maximum number of clients supported for tracking the IP address in the system
  128
Maximum number of dynamic VLANs that can be allowed using MVRP
  256
Maximum number of nexthops per IP ECMP group
    1
Maximum number of IP neighbors (IPv4+IPv6) supported in the system
 1024
Maximum number of IPv4 neighbors(# of ARP entries) supported in the system
 1024
Maximum number of IPv6 neighbors(# of ND entries) supported in the system
  512
Maximum number of L2 MAC addresses supported in the system
 8192
Maximum number of L3 Groups for IP Tunnels and ECMP Groups
    1
Maximum number of L3 Destinations for Routes, Nexthops in Tunnels and ECMP groups
 1024
Maximum number of configurable LAG ports
    8
Maximum number of members supported by a LAG port
    8
Maximum number of VLANs across ports allowed in loop-protect
 3328
Maximum number of IGMP/MLD groups supported
```

```
  512
Maximum number of IGMP/MLD snooping groups supported
  512
Maximum number of Mirror Sessions configurable in a system
    4
Maximum number of enabled Mirror Sessions in a system
    4
Maximum number of mstp instances configurable in a system
   16
Maximum number of Clients that can be authenticated on a port
   32
Maximum number of Device Profiles allowed to be created on the system
    8
Maximum number of Port Access Roles allowed to be created on the system
   32
Maximum number of MAC Address that can be authorized on a port
   32
Maximum number of Port Access Role VLAN IDs allowed to be created on the system
   50
Maximum number of Port Access Role VLAN names allowed to be created on the system
   50
Maximum number of RBAC rules per user group
 1024
Maximum number of RPVST VLANs configurable on the system
   16
Maximum number of RPVST VPORTs supported in a system
  512
Maximum number of SVIs supported in the system
   16
Maximum number of routes (IPv4+IPv6) on the system
  512
Maximum number of IPv4 routes on the system
  512
Maximum number of IPv6 routes on the system
  512
Maximum number of VLANs supported in the system
  512

System Capacities:
Capacities Name
Value
-------------------------------------------------------------------------------
--------
Maximum number of Access Control Entries configurable in a system
 4096
Maximum number of Access Control Lists configurable in a system
  512
Maximum number of class entries configurable in a system
 4096
Maximum number of classes configurable in a system
  512
Maximum number of entries in an Access Control List
 1024
Maximum number of entries in a class
 1024
Maximum number of entries in a policy
   64
Maximum number of classifier policies configurable in a system
  512
Maximum number of policy entries configurable in a system
 4096
Maximum number of clients supported for tracking the IP address in the system
```

```
  128
Maximum number of dynamic VLANs that can be allowed using MVRP
  256
Maximum number of nexthops per IP ECMP group
    1
Maximum number of IP neighbors (IPv4+IPv6) supported in the system
 1024
Maximum number of IPv4 neighbors(# of ARP entries) supported in the system
 1024
Maximum number of IPv6 neighbors(# of ND entries) supported in the system
  512
Maximum number of L2 MAC addresses supported in the system
 8192
Maximum number of L3 Groups for IP Tunnels and ECMP Groups
    1
Maximum number of L3 Destinations for Routes, Nexthops in Tunnels and ECMP groups
 1024
Maximum number of configurable LAG ports
    8
Maximum number of members supported by a LAG port
    8
Maximum number of VLANs across ports allowed in loop-protect
 3328
Maximum number of IGMP/MLD groups supported
  512
Maximum number of IGMP/MLD snooping groups supported
  512
Maximum number of Mirror Sessions configurable in a system
    4
Maximum number of enabled Mirror Sessions in a system
    4
Maximum number of mstp instances configurable in a system
   16
Maximum number of Clients that can be authenticated on a port
   32
Maximum number of Device Profiles allowed to be created on the system
    8
Maximum number of Port Access Roles allowed to be created on the system
   32
Maximum number of MAC Address that can be authorized on a port
   32
Maximum number of Port Access Role VLAN IDs allowed to be created on the system
   50
Maximum number of Port Access Role VLAN names allowed to be created on the system
   50
Maximum number of RBAC rules per user group
 1024
Maximum number of RPVST VLANs configurable on the system
   16
Maximum number of RPVST VPORTs supported in a system
  512
Maximum number of SVIs supported in the system
   16
Maximum number of routes (IPv4+IPv6) on the system
  512
Maximum number of IPv4 routes on the system
  512
Maximum number of IPv6 routes on the system
  512
Maximum number of VLANs supported in the system
  512
```

```
switch# show capacities

System Capacities:
Capacities Name
Value
-------------------------------------------------------------------------------
--------
Maximum number of Access Control Entries configurable in a system
 4096
Maximum number of Access Control Lists configurable in a system
  512
Maximum number of class entries configurable in a system
 4096
Maximum number of classes configurable in a system
  512
Maximum number of entries in an Access Control List
 1024
Maximum number of entries in a class
 1024
Maximum number of entries in a policy
   64
Maximum number of classifier policies configurable in a system
  512
Maximum number of policy entries configurable in a system
 4096
Maximum number of clients supported for tracking the IP address in the system
  128
Maximum number of dynamic VLANs that can be allowed using MVRP
  256
Maximum number of nexthops per IP ECMP group
    1
Maximum number of IP neighbors (IPv4+IPv6) supported in the system
 1024
Maximum number of IPv4 neighbors(# of ARP entries) supported in the system
 1024
Maximum number of IPv6 neighbors(# of ND entries) supported in the system
  512
Maximum number of L2 MAC addresses supported in the system
 8192
Maximum number of L3 Groups for IP Tunnels and ECMP Groups
    1
Maximum number of L3 Destinations for Routes, Nexthops in Tunnels and ECMP groups
 1024
Maximum number of configurable LAG ports
    8
Maximum number of members supported by a LAG port
    8
Maximum number of VLANs across ports allowed in loop-protect
 3328
Maximum number of IGMP/MLD groups supported
  512
Maximum number of IGMP/MLD snooping groups supported
  512
Maximum number of Mirror Sessions configurable in a system
    4
Maximum number of enabled Mirror Sessions in a system
    4
Maximum number of mstp instances configurable in a system
   16
Maximum number of Clients that can be authenticated on a port
   32
Maximum number of Device Profiles allowed to be created on the system
```

```
    8
Maximum number of Port Access Roles allowed to be created on the system
   32
Maximum number of MAC Address that can be authorized on a port
   32
Maximum number of Port Access Role VLAN IDs allowed to be created on the system
   50
Maximum number of Port Access Role VLAN names allowed to be created on the system
   50
Maximum number of RBAC rules per user group
 1024
Maximum number of RPVST VLANs configurable on the system
   16
Maximum number of RPVST VPORTs supported in a system
  512
Maximum number of SVIs supported in the system
   16
Maximum number of routes (IPv4+IPv6) on the system
  512
Maximum number of IPv4 routes on the system
  512
Maximum number of IPv6 routes on the system
  512
Maximum number of VLANs supported in the system
  512

System Capacities:
Capacities Name
Value
-------------------------------------------------------------------------------
--------
Maximum number of Access Control Entries configurable in a system
 4096
Maximum number of Access Control Lists configurable in a system
  512
Maximum number of class entries configurable in a system
 4096
Maximum number of classes configurable in a system
  512
Maximum number of entries in an Access Control List
 1024
Maximum number of entries in a class
 1024
Maximum number of entries in a policy
   64
Maximum number of classifier policies configurable in a system
  512
Maximum number of policy entries configurable in a system
 4096
Maximum number of clients supported for tracking the IP address in the system
  128
Maximum number of dynamic VLANs that can be allowed using MVRP
  256
Maximum number of nexthops per IP ECMP group
    1
Maximum number of IP neighbors (IPv4+IPv6) supported in the system
 1024
Maximum number of IPv4 neighbors(# of ARP entries) supported in the system
 1024
Maximum number of IPv6 neighbors(# of ND entries) supported in the system
  512
Maximum number of L2 MAC addresses supported in the system
```

```
 8192
Maximum number of L3 Groups for IP Tunnels and ECMP Groups
    1
Maximum number of L3 Destinations for Routes, Nexthops in Tunnels and ECMP groups
 1024
Maximum number of configurable LAG ports
    8
Maximum number of members supported by a LAG port
    8
Maximum number of VLANs across ports allowed in loop-protect
 3328
Maximum number of IGMP/MLD groups supported
  512
Maximum number of IGMP/MLD snooping groups supported
  512
Maximum number of Mirror Sessions configurable in a system
    4
Maximum number of enabled Mirror Sessions in a system
    4
Maximum number of mstp instances configurable in a system
   16
Maximum number of Clients that can be authenticated on a port
   32
Maximum number of Device Profiles allowed to be created on the system
    8
Maximum number of Port Access Roles allowed to be created on the system
   32
Maximum number of MAC Address that can be authorized on a port
   32
Maximum number of Port Access Role VLAN IDs allowed to be created on the system
   50
Maximum number of Port Access Role VLAN names allowed to be created on the system
   50
Maximum number of RBAC rules per user group
 1024
Maximum number of RPVST VLANs configurable on the system
   16
Maximum number of RPVST VPORTs supported in a system
  512
Maximum number of SVIs supported in the system
   16
Maximum number of routes (IPv4+IPv6) on the system
  512
Maximum number of IPv4 routes on the system
  512
Maximum number of IPv6 routes on the system
  512
Maximum number of VLANs supported in the system
  512
```

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>`

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 **vrrp** for which to display capacities, values, and status. Required.

Examples

Showing the system capacities status for all features:

```
switch# show capacities-status

System Capacities Status
Capacities Status Name                                                    Value
Maximum
-------------------------------------------------------------------------------
----
Number of Access Control Entries currently configured                      0    4096
Number of Access Control Lists currently configured                        0     512
Number of class entries currently configured                               0    4096
Number of classes currently configured                                     0     512
Number of policies currently configured                                    0     512
Number of policy entries currently configured                              0    4096
Number of dynamic VLANs currently learnt using MVRP                        0     256
Number of IP neighbor (IPv4+IPv6) entries                                  1    1024
Number of IPv4 neighbor(ARP) entries                                       1    1024
Number of IPv6 neighbor(ND) entries                                        0     512
Number of L3 Groups for IP Tunnels and ECMP Groups currently configured    0       1
Number of L3 Destinations for Routes, Nexthops in ECMP groups and
   Tunnels currently configured                                            0    1024
Number of Mirror Sessions currently configured                             0       4
Number of Mirror Sessions currently enabled                                0       4
Number of mstp instances currently configured                              0      16
Number of RPVST VLANs currently configured                                 0      16
Number of routes (IPv4+IPv6) currently configured                          1     512
Number of IPv4 routes currently configured                                 1     512
Number of IPv6 routes currently configured                                 0     512
Number of VLANs currently configured                                       1     512
```

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
`feature`	Optional. Specify feature name. 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
```

Description

Shows the current domain name.

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` is not available for JL679A.

```
show environment fan
```

Description

Shows the status information for all fans and fan trays (if present) in the system.

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.
   N/A:This value is not applicable to the 6000 or 6100.
Direction: The direction of airflow through the fan. Values are:
   left-to-right:Air flows from the left of the system to the right 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 systems with fan trays for 6100 switch series:

```
switch# show environment fan
Fan information
-------------------------------------------------------------------------------
Mbr/Fan       Product  Serial Number  Speed   Direction      Status  RPM
              Name
-------------------------------------------------------------------------------
1/1           N/A      N/A            N/A     left-to-right  ok      N/A
```

```
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
```

Description

Shows state and status information for all the configurable LEDs in the system.

Example

Showing state and status for LED:

```
switch# show environment led
Mbr/Name       State      Status
------------------------------
1/locator      off        ok
```

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-supply

```
show environment power-supply
```

Description

Shows status information about all power supplies in the switch.

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`	The status of the power supply. Values are: ▪ **OK**:Power supply is operating normally. ▪ **OK***: Power supply is operating normally, but it is the only power supply in the

Parameter	Description
	chassis. One power supply is not sufficient to supply full power to the switch. When this value is shown, the output of the command also shows a message at the end of the displayed data. ■ **Absent**: No power supply is installed in the specified slot. ■ **Input fault**: The power supply has a fault condition on its input. ■ **Output fault**: The power supply has a fault condition on its output. ■ **Warning**: The power supply is not operating normally. ■ **Wattage Maximum**: Shows the maximum amount of wattage that the power supply can provide.

Example

Showing the output when only one power supply is installed in the switch:

```
switch# show environment power-supply
         Product  Serial                PSU           Wattage
Mbr/PSU  Number   Number                Status        Maximum
-------------------------------------------------------------
1/1      N/A      N/A                   OK            500
```

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 temperature

```
show environment temperature [detail]
```

Description

Shows the temperature information from sensors in the switch that affect fan control.

Parameter	Description
`detail`	Shows detailed information from each temperature sensor.

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

Showing current temperature information for a 6100 switch:

```
switch# show environment temperature
Temperature information
------------------------------------------------------------------------------
                                                    Current
Mbr/Slot-Sensor                 Module Type       temperature  Status
------------------------------------------------------------------------------
1/1-COMe-Daughter-Boar          line-card-module     66.45 C    normal
1/1-PCIE-Switch                 line-card-module     95.82 C    normal
1/1-Processor                   line-card-module     00.00 C    fault
1/1-Switch-ASIC                 line-card-module     116.36 C   emergency
1/1-Switch-ASIC-Internal        line-card-module     108.25 C   critical
1/2-COMe-Daughter-Boar          line-card-module     67.29 C    normal
1/2-PCIE-Switch                 line-card-module     95.82 C    normal
1/2-Processor-1                 line-card-module     72.92 C    normal
1/2-Processor-2                 line-card-module     73.05 C    normal
1/2-Switch-ASIC                 line-card-module     97.41 C    normal
1/2-Switch-ASIC-Internal        line-card-module     97.62 C    normal
...
```

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
`-e <EVENT-ID>`	Shows the event logs for the specified event ID. Event ID range: 101 through 99999.
`-s {emergency | alert | critical | error | warning | notice | info | debug}`	Shows the event logs for the specified severity. Select the severity from the following list: ■ `emergency`: Displays event logs with severity emergency only. ■ `alert`: Displays event logs with severity alert and above. ■ `critical`: Displays event logs with severity critical and above. ■ `error`: Displays event logs with severity error and above. ■ `warning`: Displays event logs with severity warning and above. ■ `notice`: Displays event logs with severity notice and above. ■ `info`: Displays event logs with severity info and above. ■ `debug`: Displays event logs with all severities.
`-r`	Shows the most recent event logs first.
`-a`	Shows all event logs, including those events from previous boots.
`-n <COUNT>`	Displays the specified number of event logs.
`-c {lldp | ospf | ...}`	Shows the event logs for the specified event category. Enter `show event -c` for a full listing of supported categories with descriptions.
`-d {lldpd | bgpd | fand | ...}`	Shows the event logs for the specified process. Enter `show event -d` 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 front-panel-security status

```
show front-panel-security status
```

Description

Displays the configuration status of the front panel factory reset feature and the time stamp of the first occurrence of factory reset using the reset button.

Example

Displays the status of the front panel factory reset feature:

```
switch# show front-panel-security status
Front panel factory reset                    : enabled
First occurrence of front-panel factory reset : Wed 2023-09-06 02:57:50 +08
```

Displays the status of the front panel factory reset feature:

```
switch# show front-panel-security status
Front panel factory reset                    : enabled but unsupported
First occurrence of front-panel factory reset : NA
```

If the status of the feature is displayed as **enabled but unsupported**, then users should issue the **allow-unsafe-updates** command and reboot the switch.

```
switch# config
switch(config)# allow-unsafe-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 features that use this command, refer to the Fundamentals Guide for your switch model.

Command History

Release	Modification
10.13.1000	Command introduced

Command Information

Platforms	Command context	Authority
6000 6100	Manager (#)	Administrators or local user group members with execution rights for this command.

show hostname

```
show hostname
```

Description

Shows the current host name.

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
```

Description

Shows information about the software in the primary and secondary images.

Example

Showing the primary and secondary images on a 6100 switch:

```
switch(config)# show images
--------------------------------------------------------------------------------
AOS-CX Primary Image
--------------------------------------------------------------------------------
Version : PL.10.06.0002E
Size    : 243 MB
Date    : 2020-11-25 22:00:47 PST
```

```
SHA-256 : 61fe9233b2c842e8ac1731ad46949bd63e269c5c72d69290932ef19c1ebb0730

--------------------------------------------------------------------------------
AOS-CX Secondary Image
--------------------------------------------------------------------------------
Version : PL.10.07.0000E-201-gba0c336
Size    : 271 MB
Date    : 2020-11-25 21:09:08 UTC
SHA-256 : 2fdfc646a8013efcca75729584bbb0fa54604086bad3f46e1c5d4e706b8b30ee

Default Image : primary
Boot Profile Timeout : 2 seconds

--------------------------------------------------------------------------------
Management Module 1/1 (Active)
--------------------------------------------------------------------------------
Active Image       : primary
Service OS Version : PL.01.07.0003-internal
BIOS Version       : PL.01.0001
```

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 module

```
show module
```

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.

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 is the active 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.
`Failed`
The switch has experienced an error and failed.
`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 a 6100 switch:

```
switch# show module

Management Modules
==================

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL678A  6100F 24G 4SFP+ Swch               SG0ZKW600P Active (local)

Line Modules
============

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL678A  6100F 24G 4SFP+ Swch               SG0ZKW600P Ready

Management Modules
==================

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL678A  6100F 24G 4SFP+ Swch               SG0ZKW600P Active (local)

Line Modules
============

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL678A  6100F 24G 4SFP+ Swch               SG0ZKW600P Ready
```

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]`

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 `show running-config` command, followed by a space, followed by a question mark (?).
all	Shows all default values for the current running configuration.

Examples

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version AOS-CX PL.10.06.0001-346-g56a12a8f4cf15
!export-password: default
ntp enable
!
!
!
!
ssh server vrf default
vlan 1
spanning-tree
spanning-tree instance 1 vlan 1,2,4-10
interface 1/1/1
    no shutdown
```

```
    vlan access 1
    portfilter 1/1/2-1/1/3

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
snmp-server community public
snmp-server host 1.1.1.1 inform version v2c
snmp-server host 1.1.1.1 trap version v2c
snmpv3 context A vrf default
!
!
!
!
!
https-server vrf default
```

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 PL.10.06.0001-346-g56a12a8f4cf15
!export-password: default
!
!
!
!
ssh server vrf default
vlan 1
spanning-tree
interface 1/1/1
    no shutdown
    vlan access 1
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
!
!
!
!
!
https-server vrf default
switch#
switch#                                                PL.10.06.0001-346-
g56a12a8f4cf15
!export-password: default
!
!
!
!
ssh server vrf default
vlan 1
spanning-tree
interface 1/1/1
    no shutdown
    vlan access 1
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
!
!
!
!
!
https-server vrf default
switch#
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 (#)	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
    no shutdown
    description Example interface
vlan access 1
    exit
```

Showing the current running configuration for the in-band management interface:

```
switch(config)# interface vlan 1
switch(config-if-vlan)#description IN-BAND Management Interface
switch(config-if-vlan)#ip dhcp
switch(config-if-vlan)#no shutdown
switch(config-if-vlan)#end
switch#
```

Showing the current running configuration for the in-band management interface without DHCP:

```
switch(config)# interface vlan 1
switch(config-if-vlan)#description IN-BAND Management Interface
switch(config-if-vlan)#no ip dhcp
switch(config-if-vlan)#ip address 192.168.10.1/24
switch(config-if-vlan)#no shutdown
```

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

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)#
```

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` or a child of `config`. 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
`json`	Display output in JSON format.

Examples

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]`

Description

Shows general status information about the system.

Parameter	Description
`serviceos password-prompt`	Shows the Service OS password prompt status.

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.

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      : XXXXXXXXXX
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
```

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]
```

Description

Shows the system resource utilization data.

Parameter	Description
`all`	Shows the resource utilization data for the entire switch.

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
```

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 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
```

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 output of this command includes **CPU usage(% average over 1 minute)** and **CPU usage(% average over 5 minute)**.
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
`basic`	Specifies showing a basic set of information.

Parameter	Description
<FEATURE>	Specifies the name of a feature. For a list of feature names, enter the `show tech` command, followed by a space, followed by a question mark (?).
`local-file`	Shows the output of the `show tech` 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
```

Description

Shows the USB port configuration and mount settings.

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
```

Description

Shows version information about the network operating system software, service operating system software, and BIOS.

Example

Showing version information for a 6100 switch:

```
switch(config)# show version
------------------------------------------------------------------------------
AOS-CX
(c) Copyright 2017-2022 Hewlett Packard Enterprise Development LP
------------------------------------------------------------------------------
Version      : PL.10.xx.xxxxx
Build Date   : 2022-05-27 17:00:46 PDT
Build ID     : AOS-CX:PL©10.xx.xxxxx:9e8bf51170a6:202012062115
Build SHA    : 9e8bf51170a602370f12e0bde814e8d8f49bf706
Active Image : secondary

Service OS Version : PL.10.xx.xxxxx
BIOS Version       : PL.01.0002
```

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.

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.

Parameter	Description
`vrf <VRF-NAME>`	Specifies the Telnet sessions for a specific VRF.
`all-vrfs`	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
```

Showing the Telnet sessions on all VRFs:

```
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.

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 **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 all other 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
`notify <event|debug|all>`	Specifies the type of log notification. ■ **Event:** Displays the event log messages. (Default) ■ **Debug:** Displays the debug log messages. ■ **All:** Displays both event and debug log messages.
`severity <level>`	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).
`filter <keyword>`	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
`notify <event|debug|all>`	Specifies the type of log notification. ▪ **Event:** Displays the event log messages. (Default) ▪ **Debug:** Displays the debug log messages. ▪ **All:** Displays both event and debug log messages.
`severity <level>`	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).
`filter <keyword>`	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>}
```

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 dsrport 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 **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.

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 **radius** is available. 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 **aaa group server** and servers are added to a server group with the command **server**.

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. By default, the username found in the certificate field UserPrincipalName (UPN) is used for authorization on the RADIUS serer. When this parameter is omitted, **authorization radius** is still the assumed active setting.
<CERT-FIELD>	Selects which certificate username field is to be used for authorization.

Parameter	Description
	▪ Specify **user_pincipal_name** to use the certificate UserPrincipalName (UPN) field. This is the default. ▪ Specify **common_name** to use the certificate CommonName (CN) field. When this parameter is omitted, **user_pincipal_name** is assumed.

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
`authorization radius`	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 **authorization radius** parameter
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.

Chapter 99
UDLD commands

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>]`

Description

Displays UDLD information for all interfaces or for a specific interface.

Parameter	Description
`interface <INTERFACE-NAME>`	Specifies the name of a logical interface on the switch, which can be: ■ An Ethernet interface associated with a physical port. Use the format **member/slot/port** (for example, **1/3/1**). ■ 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.

Examples

Displaying all UDLD information:

```
switch# show udld

Abbreviations:
 VTF - Verify-then-forward    FTV - Forward-then-verify
 NOR - RFC 5171 normal        AGG - RFC 5171 aggresive

------------------------------------------------------------------------
Interface  UDLD      UDLD      UDLD           UDLD    Mode  Interval
           Config    State     Substate       Link
------------------------------------------------------------------------
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       Rx       Rx          Rx          Transitions
         Pkts     Pkts     Pkts disc.  Pkts drop.
-----------------------------------------------------------------
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
 Version: Aruba OS
 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 aggresive

------------------------------------------------------------------------------
-------------------------------------------------
Interface  UDLD      UDLD      UDLD           UDLD     Mode  Interval  Retries  Tx
      Rx       Rx          Rx          Transitions
           Config    State     Substate       Link
Pkts     Pkts     Pkts disc.  Pkts drop.
------------------------------------------------------------------------------
-------------------------------------------------
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
disable	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).

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. Aruba 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 (ERPS is not supported on the 6000 or 6100). 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. Aruba 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.

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 or 1000 ms to 90000 ms for the 6000 and 6100 Switch Series (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
aruba-os *{verify-then-forward | forward-then-verify}*	Selects the ArubaOS mode to use. Use this mode when interconnecting with HPE PVOS/Brocade/Foundry switches.
verify-then-forward	In this mode: ■ Interfaces start as unblocked. ■ Once an interface is determined to be bidirectional, it is blocked if the retry limit is reached without receiving any UDLD packets. ■ Interfaces automatically unblock if a UDLD packet is received. ■ On failover, the UDLD state does not change if the (interval * retries) time is around 6 seconds.
forward-then-verify	In this mode: ■ Interfaces start as unblocked.

Parameter	Description
	▪ Interfaces transition to the unblocked state when receiving UDLD packets. ▪ Once an interface is determined to be bidirectional, it is blocked if the retry limit is reached without receiving any UDLD packets. ▪ Interfaces automatically unblock if a UDLD packet is received.
`rfc5171 <RFC5171-MODE>`	Selects the RFC5171 mode to use. Use this mode when interconnecting with third-party switches.
`normal`	In this mode: ▪ Interfaces start as unblocked. ▪ 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. ▪ Interfaces automatically unblock if a UDLD packet is received.
`aggressive`	In this mode: ▪ Interfaces start as unblocked. ▪ 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). ▪ Interfaces implement a limited/reduced errDisabled recovery 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
<COUNT>	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.

Chapter 100
UFD (Uplink Failure Detection) commands

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
<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 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-<ID>`	Administrators or local user group members with execution rights for this command.

show capacities ufd

```
show capacities ufd
show capacities-status ufd
```

Description

Command **show capacities ufd** shows UFD session capacity. Command **show capacities-status ufd** shows UFD session capacity and the number of UFD sessions configured.

Example

Showing UFD session capacity:

```
switch# show capacities ufd

System Capacities: Filter UFD
Capacities Name                                                                  Value
--------------------------------------------------------------------------------
---
Maximum number of Uplink Failure Detection sessions configurable in a system  128
```

Showing UFD session capacity and the number of UFD sessions configured:

```
switch(config)# show capacities-status ufd

System Capacities Status: Filter UFD
Capacities Status Name                                                    Value
Maximum
------------------------------------------------------------------------------
---
Number of Uplink Failure Detection sessions currently configured          1    128
```

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	Operator (>) or Manager (#)	Operators 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 ufd

```
show running-config ufd
```

Description

Shows the running configuration for UFD.

Example

Showing the UFD portion of running configuration information:

```
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)#

switch# show running-config ufd
Current configuration:
ufd enable

ufd session-id 1
    delay up 10
    delay down 10
```

```
    links-to-monitor 1/1/1,1/1/2
    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	Operator (>) or Manager (#)	Operators 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 ufd

```
show-tech ufd
```

Description

Executes the **show ufd** command followed by the **show running-config ufd** command.

Example

Running the **show ufd** command followed by the **show running-config ufd** command:

```
switch# show tech ufd
======================================================
Show Tech executed on Tue Nov 23 11:32:08 2021
======================================================
======================================================
[Begin] Feature ufd
======================================================


********************************
Command : show ufd
********************************
Global UFD Status : Enabled

UFD session-id                  : 10
UFD Links-to-Monitor status     : Up
Up Delay                        : 20 sec
Down Delay                      : 10 sec
Links-to-Monitor                : None
Links-to-Disable                : None
Last Links-to-Monitor Down Time  : None
```

```
UFD session-id                    : 20
UFD Links-to-Monitor status       : Up
Up Delay                          : 0 sec
Down Delay                        : 0 sec
Links-to-Monitor                  : None
Links-to-Disable                  : None
Last Links-to-Monitor Down Time   : None

********************************
Command : show running-config ufd
********************************
ufd enable
ufd session-id 10
    delay down 10
    delay up 20
    exit
ufd session-id 20
    exit
=====================================================
[End] Feature ufd
=====================================================


=====================================================
Show Tech commands executed successfully
=====================================================
```

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

show ufd

`show ufd [session-id <ID>]`

Description

Shows information on all UFD sessions or the specified UFD session.

Parameter	Description
<ID>	Specifies an existing UFD session ID. Range: 1 to 128.

Example

Showing information on all configured UFD sessions:

```
switch# show ufd
Global UFD Status : Enabled

UFD session-id                    : 1
UFD Links-to-Monitor status       : Up
Up Delay                          : 10 sec
Down Delay                        : 10 sec
Links-to-Monitor                  : 1/1/1,1/1/2
Links-to-Disable                  : 1/1/11,1/1/12
Last Links-to-Monitor Down Time   : 2021-11-03 15:22:05:37

UFD session-id                    : 2
UFD Links-to-Monitor status       : Up
Up Delay                          : 5 sec
Down Delay                        : 5 sec
Links-to-Monitor                  : lag18-lag20
Links-to-Disable                  : 1/1/3-1/1/5
Last Links-to-Monitor Down Time   : 2021-11-01 12:14:42:56
```

Showing information on UFD session 2:

```
switch# show ufd session 2

UFD session-id                    : 2
UFD Links-to-Monitor status       : Up
Up Delay                          : 5 sec
Down Delay                        : 5 sec
Links-to-Monitor                  : lag18-lag20
Links-to-Disable                  : 1/1/3-1/1/5
Last Links-to-Monitor Down Time   : 2021-11-01 12:14:42:56
```

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

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: ■ dns (53): Domain Name Service ■ ntp (123): Network Time Protocol ■ netbios-ns (137): NetBIOS Name Service ■ netbios-dgm (138): NetBIOS Datagram Service ■ radius (1812): Remote Authentication Dial-In User Service ■ radius-old (1645): Remote Authentication Dial-In User Service ■ rip (520): Routing Information Protocol ■ snmp (161): Simple Network Management Protocol ■ snmp-trap (162): Simple Network Management Protocol ■ tftp (69): Trivial File Transfer Protocol ■ timep (37): Time Protocol

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>]
```

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.

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 apples 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: ebCD4Position 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). Similarity, 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 off 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	**adjacent-char-type-count** 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.

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>	Specifies the user name. Requirements: Must start with a lowercase or uppercase letter. Can contain numbers, lowercase, and uppercase letters. Can include only these three special characters: hyphens (-), dots (.), and underscores (_). Can have a maximum of 32 characters. Cannot be empty. Cannot be: admin, `root`, or `remote_user`. Cannot be Linux reserved names such as: `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`. **NOTE**: 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.
`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 *<CIPHERTEXT-PASSWORD>* is Base64 and is typically copied from another switch using the `show running-config` command output and then pasted into this command.

Parameter	Description
	NOTE: 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 `user` command. The ciphertext is available for copying from the `show running-config` 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.
`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

- 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-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
<GROUP-NAME>	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.

Sample matching criteria	Sample matched CLI command or specifier	Matches
`show .*`	`show accounting log`	All **show** commands
`bgp .*`	`bgp router-id 1.1.1.1`	All **bgp** 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: **ssh**, **telnet**, **https-server**, **console**. Note that **https-server** 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 **admisn1**:

```
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>*	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 *<CIPHERTEXT-PASSWORD>* is Base64 and is typically copied from another switch using the `show running-config` command output and then pasted into this command. **NOTE:** 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 `user` command. The ciphertext is available for copying from the `show running-config` 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.
`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>]`

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
<GROUP-NAME>	Narrows the **show** command output to that of the specified group, and for local user groups, adds the **User Group Rules** list.

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 **User login session** 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
```

Description

Shows all configured users and their corresponding group names.

Examples

Show the user list from a switch with only the admin user defined.

```
switch# show user-list

USER                          GROUP
-----------------------------------------------
admin                         administrators
```

Show the user list after adding a user to the operators built-in group.

```
switch# show user-list
```

```
USER                          GROUP
-----------------------------------------------
admin                         administrators
oper1                         operators
```

Show the user list after adding a user to the auditors built-in group.

```
switch# show user-list

USER                          GROUP
-----------------------------------------------
admin                         administrators
oper1                         operators
audit1                        auditors
```

Show the user list after adding a total of three users to two user-defined user groups.

```
switch# show user-list

USER                          GROUP
-----------------------------------------------
admin                         administrators
oper1                         operators
audit1                        auditors
adm1a                         admuser1
admin2-a                      admuser2
admin2-b                      admuser2
```

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-list management-interface

`show user-list management-interface`

Description

Shows a list of local users and the enabled management interfaces for each user.

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.

Examples

Showing 4100i, 6000, and 6100 switch series SVI capacity:

```
switch# show capacities svi-count
System Capacities: Filter SVI count
Capacities Name                                                    Value
-------------------------------------------------------------------------
Maximum number of SVIs supported in the system                     16
```

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 vlan

```
show vlan [<VLAN-ID>]
```

Description

Displays configuration information for all VLANs or a specific VLAN.

Parameter	Description
<VLAN-ID>	Specifies a VLAN ID.

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>`

Description

Displays the VLANs configured for a specific layer 2 interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface ID. Format: **member/slot/port**.

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 RADIUS server provided VLAN 2,3,5 as extended access VLANs (MBV):

```
switch# show vlan port 1/1/1
---------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
---------------------------------------------------------------------------
2     UserVLAN1                       access          mbv, port
3     UserVLAN2                       access          mbv
5     UserVLAN5                       access          mbv

Overriden VLAN list: 2-3,5
```

Displaying RADIUS server provided VLAN 50 as access VLAN and mode as access:

```
switch# show vlan port 1/1/1
---------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
---------------------------------------------------------------------------
50    VLAN50                          access          port-access

Overridden VLAN list: 2-3,5
```

Displaying RADIUS server provided VLAN 50 as access VLAN and mode as access, and 2,3 as extended access VLANs (MBV):

```
switch# show vlan port 1/1/1
---------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
---------------------------------------------------------------------------
2     UserVLAN1                       access          mbv
3     UserVLAN2                       access          mbv
50    VLAN50                          access          port-access

Overridden VLAN list: 2-3,5
```

Displaying RADIUS server provided mode as native-untagged, 11-14 as trunk VLANs, VLAN 11 as an access VLAN and VLAN 2, 3 as extended access VLANs (MBV):

```
switch# show vlan port 1/1/1
---------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
---------------------------------------------------------------------------
2     UserVLAN1                       access          mbv
3     UserVLAN2                       access          mbv
11    VLAN11                          native-untagged port-access
```

```
12    VLAN12                          trunk           port-access
13    VLAN13                          trunk           port-access
14    VLAN14                          trunk           port-access

Overridden VLAN list: 2-3,5
```

Displaying RADIUS server provided mode as native-tagged, 11-14 as trunk VLANs, VLAN 11 as an access VLAN and VLAN 2, 3 as extended access VLANs (MBV):

```
switch# show vlan port 1/1/1
--------------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
--------------------------------------------------------------------------------
2     UserVLAN1                       native-untagged mbv, port
3     UserVLAN2                       access          mbv
11    VLAN11                          trunk           port-access
12    VLAN12                          trunk           port-access
13    VLAN13                          trunk           port-access
14    VLAN14                          trunk           port-access

Overridden VLAN list: 3,5
```

Displaying RADIUS server provided mode as native-tagged, 3, 11-14 as trunk VLANs, VLAN 11 as an access VLAN and VLAN 2, 3 as extended access VLANs (MBV):

```
switch# show vlan port 1/1/1
--------------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
--------------------------------------------------------------------------------
2     UserVLAN1                       native-untagged mbv, port
3     UserVLAN2                       native-untagged port-access, mbv
11    VLAN11                          trunk           port-access
12    VLAN12                          trunk           port-access
13    VLAN13                          trunk           port-access
14    VLAN14                          trunk           port-access

Overridden VLAN list: 3,5
```

Displaying RADIUS server provided mode as native-tagged, 2, 11-14 as trunk VLANs, VLAN 11 as an access VLAN:

```
switch# show vlan port 1/1/1
--------------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
--------------------------------------------------------------------------------
2     UserVLAN1                       trunk           port-access
11    VLAN11                          native-tagged   port-access
12    VLAN12                          trunk           port-access
13    VLAN13                          trunk           port-access
14    VLAN14                          trunk           port-access

Overridden VLAN list: 2-3,5
```

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
```

Displaying RADIUS server provided VLANs 2,11-14 as trunk VLANs, VLAN 2 as an access VLAN, and mode as native-untagged:

```
switch# show vlan port 1/1/3
--------------------------------------------------------------------------------
VLAN  Name                            Mode            Mapping
--------------------------------------------------------------------------------
2     UserVLAN1                       native-untagged port-access
11    VLAN11                          trunk           port-access
12    VLAN12                          trunk           port-access
13    VLAN13                          trunk           port-access
14    VLAN14                          trunk           port-access

Overridden VLAN list: 1-3,5,10-14,20,30,40,50,100,200
```

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
```

Description

Displays a summary of the VLAN configuration on the switch.

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
Number of port-access VLANs: 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 (#)	Operators 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 vlan-client-presence-detect

```
system vlan-client-presence-detect
no system vlan-client-presence-detect
```

Description

Enables VNI mapped VLANs when detecting the presence of a client. When enabled, VNI mapped VLANs are *up* only if there are authenticated clients on the VLAN, or if the VLAN has statically configured ports and those ports are *up*. When not enabled, VNI mapped VLANs are always *up*.

The **no** form of this command disables detection of clients on VNI mapped VLANs.

Examples

Enabling detection of clients:

```
switch(config)# system vlan-client-presence-detect
```

Disabling detection of clients:

```
switch(config)# no system vlan-client-presence-detect
```

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
6000 6100	`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	`config`	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 . A maximum of 512 (6000, 6100 Switch Series) VLANs are supported.

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
<VLAN-ID>	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 . A maximum of 512 (6000, 6100 Switch Series) VLANs are supported.

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)# 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 trunk allowed

```
vlan trunk allowed [<VLAN-LIST> | all]
no vlan trunk allowed [<VLAN-LIST>]
```

Description

Assigns a VLAN ID to an 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 .
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)# 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)# 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)# 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>	

Examples

Assigning native VLAN ID **20** to trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
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)# 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 .

Examples

Enabling tagging on native VLAN **20** on trunk interface **1/1/2**:

```
switch(config)# interface 1/1/2
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-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-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

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 **erase all** 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 IP address of the TFTP server
- The name of the image file
- The name of the configuration file
- The Aruba Central FDQN or IPv4 address
- The HTTP proxy FDQN or IPv4 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:

Success

The ZTP operation succeeded.

One of the following is true:

- Both the running configuration and the startup configuration were updated.
- The IP address of the TFTP server was received, but the offer did not include a configuration file or a firmware image file.
- Any combination of vendor encapsulated DHCP options are received as configured, along with the firmware image and switch configuration file.
- Only vendor encapsulated DHCP options are configured and are received accordingly.

Failed - Custom startup configuration detected

The switch was booted from a configuration that is not the factory default configuration. For example, the administrator password has been set.

Failed - Timed out while waiting to receive ZTP options

Either the switch received the DHCP IPv4 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.

Failed - Detected change in running configuration

The running configuration was modified by a user while the ZTP operation was in progress.

Failed - TFTP server unreachable

The TFTP server is not reachable at the specified IP address.

Failed - TFTP server information unavailable

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.

Failed - Invalid configuration file received

Either the file transfer of the configuration file failed, or the configuration file is invalid (an error occurred while attempting to apply the configuration).

Failed - Invalid image file received

Either the file transfer of the firmware image file failed, or the firmware image file is invalid (an error occurred while verifying the image).

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 download 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                 : config_file
ZTP Status                         : In-progress - Image download and verification
Aruba Central Location             : secure.arubanetworks.com
Alternative Aruba Central Location: NA
Aruba Central Shared Token         : aruba123
Force-Provision                    : Disabled
HTTP Proxy Location                : http.proxy.arubanetworks.com
```

Showing switch image download failure after receiving ZTP options:

```
switch# show ztp information
TFTP Server                        : 10.0.0.2
Image File                         : TL_10_02_0001.swi
Configuration File                 : config_file
ZTP Status                         : Failed - Unable to download image
Aruba Central Location             : secure.arubanetworks.com
Alternative Aruba Central Location: NA
Aruba Central Shared Token         : aruba123
Force-Provision                    : Disabled
HTTP Proxy Location                : http.proxy.arubanetworks.com
```

Showing switch configuration download 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                  : config_file
```

```
ZTP Status                          : In-progress - Configuration download
Aruba Central Location              : secure.arubanetworks.com
Alternative Aruba Central Location : NA
Aruba Central Shared Token          : aruba123
Force-Provision                     : Disabled
HTTP Proxy Location                 : http.proxy.arubanetworks.com
```

Showing switch configuration download failure after receiving ZTP options:

```
switch# show ztp information
TFTP Server                         : 10.0.0.2
Image File                          : TL_10_02_0001.swi
Configuration File                  : config_file
ZTP Status                          : Failed - Unable to download configuration
Aruba Central Location              : secure.arubanetworks.com
Alternative Aruba Central Location : NA
Aruba Central Shared Token          : aruba123
Force-Provision                     : Disabled
HTTP Proxy Location                 : http.proxy.arubanetworks.com
```

Showing switch failure to update start-up configuration after downloading configuration received from ZTP options:

```
switch# show ztp information
TFTP Server                        : 10.0.0.2
Image File                         : TL_10_02_0001.swi
Configuration File                 : config_file
ZTP Status                         : Failed - Could not copy to start-up configuration
Aruba Central Location             : secure.arubanetworks.com
Alternative Aruba Central Location: NA
Aruba Central Shared Token         : aruba123
Force-Provision                    : Disabled
HTTP Proxy Location                : http.proxy.arubanetworks.com
```

In the following example, the ZTP operation succeeded, and both an image file and a configuration file were provided.

```
switch# show ztp information
TFTP Server            : 20.1.1.4
Image File             : PL_10_06_0001BT.swi
Configuration File     : bristol_maxlimit
Status                 : Success
Force-Provision        : Disabled
switch#
```

In the following example, the ZTP option succeeded. A configuration file was not provided, but an image file was provided.

```
switch# show ztp information
TFTP Server            : 20.1.1.4
Image File             : NA
Configuration File     : bristol_maxlimit
Status                 : Success
```

```
Force-Provision        : Disabled
switch#
```

In the following example, the ZTP operation failed because the TFTP server was unreachable.

```
switch# show ztp information
TFTP Server            : 20.1.1.4
Image File             : PL_10_06_0001BT.swi
Configuration File     : bristol_maxlimit
Status                 : Failed - TFTP server unreachable
Force-Provision        : Disabled
switch#
```

In the following example, the ZTP operation was stopped because the switch did not receive any options from the DHCP server for ZTP within 1 minute of receiving the IP address from the server.

```
switch## show ztp information
TFTP Server            : NA
Image File             : NA
Configuration File     : NA
Status                 : Failed - Timed out while waiting to receive ZTP options
Force-Provision        : Disabled
switch#
```

In the following example, the ZTP operation was stopped because the switch was booted from a configuration that was not the factory default configuration.

```
switch# show ztp information
TFTP Server            : 20.1.1.4
Image File             : PL_10_06_0001BT.swi
Configuration File     : bristol_maxlimit
Status                 : Failed - Custom startup configuration detected
Force-Provision        : Disabled
```

In the following example, the switch received the image file and the TFTP-sever and config file from the DHCP server for ZTP was successful:

```
switch# show ztp information
TFTP Server                       : 10.0.0.2
Image File                        : TL_10_02_0001.swi
Configuration File                : ztp.cfg
ZTP Status                        : Success
Aruba Central Location            : NA
Alternative Aruba Central Location: NA
Aruba Central Shared Token        : NA
Force-Provision                   : Disabled
HTTP Proxy Location               : NA
```

In the following example, the switch received the image file and the TFTP-sever and config file from the DHCP server entered the failed state as teh TFTP server was not reachable:

```
switch# show ztp information
TFTP Server                       : 10.0.0.2
```

```
Image File                          : TL_10_02_0001.swi
Configuration File                  : ztp.cfg
ZTP Status                          : Failed - TFTP server unreachable
Aruba Central Location              : NA
Alternative Aruba Central Location: NA
Aruba 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 (#)	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.

Usage

DHCP options received are processed independent of he current state of configuration on the switch. Previous ZTP TFTP Server, Image File, Configuration File, Aruba Central Location, and HTTP Proxy location options are cleared and the switch sends a DHCP request.

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
Aruba Central Location         : NA
Aruba 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
Aruba Central Location         : NA
Aruba 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.

Chapter 106
Support and Other Resources

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
HPE Aruba Networking Support Portal	https://networkingsupport.hpe.com/home
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

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:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
HPE Aruba Networking Hardware Documentation and Translations Portal	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm

HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/

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./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). 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.