AOS-CX 10.17 Fundamentals Guide

8100, 8320, 8325, 8360, 9300, 10000 Switch Series

Hewlett Packard Enterprise

Published: November 2025
Version: 1

Copyright Information

© Copyright 2025 Hewlett Packard Enterprise Development LP.

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

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

Notices

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

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

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

Acknowledgments

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

Contents

About this document 14
Applicable products 14
Latest version available online 14
Command syntax notation conventions 14
About the examples 15
Identifying switch ports and interfaces 16

About AOS-CX 17
AOS-CX system databases 17
Network Analytics Engine introduction 18
AOS-CX CLI 18
HPE Aruba Networking Installer mobile app 18
HPE Aruba Networking NetEdit 18
Ansible modules 19
AOS-CX Web UI 19
AOS-CX REST API 19
In-band and out-of-band management 19
SNMP-based management support 20
User accounts 20

Initial Configuration 21
Initial configuration using ZTP 21
Initial configuration using the HPE Aruba Networking Installer mobile app 22
Troubleshooting Bluetooth connections 23
Bluetooth connection IP addresses 23
Bluetooth is connected but the switch is not reachable 24
Bluetooth is not connected 24
Initial configuration using the CLI 27
Connecting to the console port 27
Connecting to the management port 28
Logging into the switch for the first time 29
Setting switch time using the NTP client 29
Configuring banners 30
Configuring in-band management on a data port 31
Using the Web UI 31
Configuring the management interface 32
IP prefix priority 32
System profiles and configurable IP prefix priority 33
IP prefix priority defaults 33
IP Prefix priority commands 33
ip prefix-priority 33
ipv6 prefix-priority 34
show ip prefix-priority 35
show ipv6 prefix-priority 36
Selecting the system profile 37
System profile commands 38
profile 38
show profiles available 40
show profile current 43

Restoring the switch to factory default settings ... 44
Limitations and considerations ... 45
REST API profile switching procedure ... 46
Management interface commands ... 46
default-gateway ... 46
ip static ... 47
nameserver ... 48
psm ... 49
show interface mgmt ... 51
show psm ... 52
NTP commands ... 53
ntp authentication ... 53
ntp authentication-key ... 53
ntp disable ... 55
ntp enable ... 55
ntp conductor ... 56
ntp server ... 57
ntp trusted-key ... 59
ntp vrf ... 60
show ntp associations ... 60
show ntp authentication-keys ... 62
show ntp servers ... 62
show ntp statistics ... 63
show ntp status ... 64

Hibernation ... 65
Hibernation commands ... 65
hibernate now ... 65
hibernate periodic ... 67
show hibernation ... 69
show running-config (hibernation) ... 70

Client probe and configuration ... 70
Client probing commands ... 71
(remote) associate profile ... 71
client-probe profile force-download ... 73
remote-server refresh interval ... 74
client-probe autogen-probe-file force-regen ... 75
autogen-enable ... 75
autogen-probe-file ... 76
show client probe autogen-probe-file ... 77
vlans ... 79
name ... 80
(local) profile ... 81
entry ... 82
probe-duration ... 84
probe-interval ... 84
probe-type ... 85
vlan-list ... 86
client probe enable ... 87
show client probe profile ... 87
show client probe statistics ... 91
clear client probe statistics ... 93
show running-config ... 93
Client-probe limitations ... 95

Telnet access **97**
Telnet commands 97
show telnet server 97
show telnet server sessions 98
telnet server 99

Interface configuration **100**
Configuring a layer 2 interface 100
Configuring a layer 3 interface 100
Single source IP address 101
Priority-based flow control (PFC) 101
(Applies to the 8325, 9300, 10000) 101
(Applies to the 8325, 9300, 10000) Asymmetric PFC 102
(Applies to the 8360) 102
Configurable flow control buffer thresholds 102
For the 8325, 9300, and 10000 series switch: 102
Flow control and lossless buffering 105
For the 8325, 9300, and 10000 series switch: 105
Requirements for proper lossless buffering: 105
For the 8360 series switch: 106
Requirements for proper lossless buffering 106
Forward error correction 107
Unsupported transceiver support 107
Configuring an interface persona 108
Modes 109
Predefined and custom persona names 110
Creating and configuring an interface persona 110
Examples 110
Modes 111
Predefined and custom persona names 111
Creating and configuring an interface persona 112
Examples 112
Monitor mode 113
Interface commands 113
allow-unsupported-transceiver 113
default interface 115
description 116
diag dsm console 117
error-control 118
flow-control 119
flow-control buffer headroom 124
flow-control buffer xoff dynamic 125
flow-control buffer xoff static 126
flow-control buffer xon 127
flow-control watchdog 128
flow-control watchdog timeout resume 130
interface 131
interface loopback 131
interface vlan 132
ip address 133
ip mtu 134
ip source-interface 135
ip tcp mss 137
ip unnumbered 138
ipv6 address 140
ipv6 source-interface 141

ipv6 tcp mss ... 142
l3-counters ... 143
mtu ... 145
persona ... 146
rate-interval ... 148
routing ... 149
show allow-unsupported-transceiver ... 150
show interface ... 151
show interface dom ... 158
show interface flow-control ... 159
show interface link-diagnostics ... 163
show interface profile ... 166
show interface statistics ... 167
show interface transceiver ... 170
show interface supported-transceivers ... 173
show interface utilization ... 177
show ip interface ... 178
show ip source-interface ... 179
show ipv6 interface ... 180
show ipv6 source-interface ... 182
show system interface-group ... 183
show system interface-profile ... 185
shutdown ... 185
speed ... 186
split ... 189
system interface-group ... 193
system interface-profile ... 194
DSM commands ... 196
clear dsm statistics ... 196
diag dsm console ... 197
dsm ... 198
erspan ... 198
ipfix ... 199
dsm uplink-to-uplink ... 200
workload-migration ... 200
show dsm ... 201
show dsm erspan ... 202
show dsm ipfix ... 202
show dsm uplink-to-uplink ... 203
show dsm interface statistics ... 203
show dsm redirect vlan ... 204
show dsm statistics ... 205
show dsm vrf ... 206
show dsm workload-migration ... 207

Subinterfaces ... 209
Configuring subinterfaces ... 209
Subinterface in a router-on-a-stick deployment ... 210
Subinterface commands ... 210
encapsulation dot1q ... 211
interface ... 212
show capacities subinterface ... 213
show interface ... 214

Source interface selection ... 216
Source-interface selection commands ... 216

ip source-interface 216
ipv6 source-interface dns 218
ipv6 source-interface 219
show ip source-interface 221
show ipv6 source-interface 223
show running-config 225

VLANs 228

Precision Time Protocol (PTP) 229
Best master clock algorithm 230
Configuration examples 231
Configuration recommendations 235
PTP CoPP class configuration recommendations 235
Configuration recommendations for a boundary clock 235
QoS prioritization configuration recommendations for a transparent clock 235
General guidelines for PTP IPv4 multicast 236
Expected behavior of PTP with VSX (boundary clock) 236
Unsupported/not-Supported PTP and VSX configurations 237
PTP on VSX keepalive interface 237
Use cases 237
Use case: PTP – IPv4 over L2 spine leaf topology 238
Use case: PTP – L3 spine leaf topology 239
Use case: PTP-VSX Multicast 240
Use case: PTP TC VSX, BC VSF Topology connected via MCLAG 241
PTP commands 243
clear ptp statistics 243
clock-domain 243
clock-step 244
enable 245
ip source-interface 246
mode (PTP) 247
multicast-address 249
priority1 250
priority2 251
ptp announce-interval 252
ptp announce-timeout 253
ptp clock-source-only 255
ptp delay-req-interval 256
ptp enable 257
ptp lag-role 258
ptp neighbor-propagation-delay-threshold 259
ptp pdelay-req-interval 260
ptp peer ip 261
ptp peer-to-peer vlan 262
ptp profile 263
ptp sync-interval 265
ptp sync-timeout 266
ptp vlan 268
show ptp clock 269
show ptp foreign-clock-sources 271
show ptp interface 272
show ptp interface vlan status 276
show ptp parent 277
show ptp statistics 278
show ptp statistics vlan 280

show ptp time-property 281
show running-config ptp 282
transport-protocol 283
vsx-sync ptp-global 284
SyncE commands 285
esmc enable 285
esmc transmit-only 286
show synce interface 287
show synce status 289
synce 290
synce hold-off-time 291
synce initial-quality-level 292
synce network-type 294
synce priority 295
synce quality-mode 296
synce wait-to-restore 296

Audio-Video Bridging (AVB) 297
MSRP timer configuration 298
QoS Configuration 299
AVB commands 300
avb 300
clear msrp statistics 301
enable 301
max fan in ports 302
msrp 303
msrp timer join 304
msrp timer leave 304
msrp timer leaveall 305
show avb domain 306
show avb interface 307
show msrp interface 308
show msrp statistics 309
show msrp state 310
show msrp streams 311
show msrp streams statistics 312
show running-config avb 312
vlan 313

Configuration and firmware management 315
Upgrade and downgrade scenarios 315
Upgrades 315
Downgrades 315
Limitations 315
REST Use Case Examples 316
Hot-patch software 322
Checkpoints 324
Checkpoint types 324
Maximum number of checkpoints 324
User generated checkpoints 324
System generated checkpoints 325
Supported remote file formats 325
Rollback 325
Checkpoint auto mode 325
Testing a switch configuration in checkpoint auto mode 326
Checkpoint commands 326

checkpoint auto ... 326
checkpoint auto confirm ... 327
checkpoint diff ... 328
checkpoint post-configuration ... 331
checkpoint post-configuration timeout ... 332
checkpoint rename ... 332
checkpoint rollback ... 333
copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL> ... 334
copy checkpoint <CHECKPOINT-NAME> {running-config | startup-config} ... 335
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL> ... 336
copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME> ... 336
copy <REMOTE-URL> startup-config|running-config ... 337
copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>} ... 339
copy {running-config | startup-config} <REMOTE-URL> ... 340
copy {running-config | startup-config} <STORAGE-URL> ... 342
copy startup-config running-config ... 343
copy <STORAGE-URL> running-config ... 343
erase ... 345
show checkpoint <CHECKPOINT-NAME> ... 346
show checkpoint <CHECKPOINT-NAME> hash ... 348
show checkpoint post-configuration ... 349
show checkpoint ... 349
show checkpoint date ... 350
show running-config hash ... 351
show startup-config hash ... 352
write memory ... 353
Boot commands ... 353
boot set-default ... 353
boot system ... 354
show boot-history ... 356
Firmware management commands ... 358
copy {primary | secondary} <REMOTE-URL> ... 358
copy {primary | secondary} <FIRMWARE-FILENAME> ... 359
copy primary secondary ... 360
copy <REMOTE-URL> ... 361
copy secondary primary ... 363
copy <STORAGE-URL> ... 363
copy hot-patch ... 364
hot-patch ... 365
show hot-patch ... 367
gNMI commands ... 368
crypto pki application gnmi certificate ... 368
gnmi vrf ... 368
show gnmi ... 369

Dynamic Segmentation ... 371

SNMP ... 372
Configuring SNMP ... 372

HPE Aruba Networking Central integration ... 374
Connecting to HPE Aruba NetworkingCentral ... 374
Custom CA certificate ... 374
Support mode in HPE Aruba Networking Central ... 375
One Touch Provisioning ... 375
HPE Aruba Networking Central commands ... 377

hpe-anw-central 377
hpe-anw-central support-mode 378
configuration-lockout central managed 379
diag-dump rest basic 380
disable 381
enable 382
location-override 383
location-override-alternative 384
show hpe-anw-central 386
show running-config current-context 389
Troubleshooting 390
Prerequisites 390
Troubleshooting Scenarios 390
Scenario: Central location discovery 390
Scenario: Central connectivity 393
Scenario: Activate connectivity 401
Scenario: Central remote console shell 401
Scenario: Central disconnection timeout 408
Related features 411

Port filtering 412
Port filtering commands 412
portfilter 412
show portfilter 414

DNS 416
DNS client 416
Configuring the DNS client 416
DNS client commands 418
ip dns domain-list 418
ip dns domain-name 419
ip dns host 419
ip dns server address 420
show ip dns 421

Device discovery and configuration 424
Device Profile Usage Considerations 424
aaa authentication port-access allow-cdp-auth 425
aaa authentication port-access allow-cdp-bpdu 426
aaa authentication port-access allow-cdp-proxy-logoff 427
aaa authentication port-access allow-lldp-bpdu 428
enable 430
LLDP 431
LLDP agent 432
LLDP MED support 434
LLDP EEE 434
Configuring the LLDP agent 434
LLDP commands 435
clear lldp neighbors 435
clear lldp statistics 436
lldp 436
lldp dot3 437
lldp dot3 mfs 438
lldp holdtime-multiplier 438
lldp management-address vlan 439
lldp management-ip-address 440

lldp management-ipv6-address 441
lldp med 442
lldp med location 443
lldp receive 445
lldp reinit 446
lldp select-tlv 447
lldp timer 448
lldp tlv-enable 449
lldp transmit 450
lldp txdelay 451
lldp trap enable 452
show lldp configuration 454
show lldp configuration mgmt 456
show lldp local-device 456
show lldp neighbor-info 458
show lldp neighbor-info detail 461
show lldp neighbor-info mgmt 464
show lldp statistics 465
show lldp statistics mgmt 467
show lldp tlv 467
Cisco Discovery Protocol (CDP) 468
CDP support 468
CDP commands 469
cdp 469
clear cdp counters 470
clear cdp neighbor-info 470
show cdp 471
show cdp neighbor-info 472
show cdp traffic 473
show cdp voice-vlan mode 473

Zero Touch Provisioning 475
ZTP support 475
Setting up ZTP on a trusted network 477
ZTP using USB 478
ZTP process during switch boot 479
ZTP VSF switchover support 480
ZTP commands 480
show ztp information 480
ztp force provision 484

Thermal Management 485
Thermal management support 485
Transceiver Thermal Management 486

Switch system and hardware commands 489
allow-non-failsafe-updates 489
bluetooth disable 489
bluetooth enable 490
clear events 491
clear ip errors 492
console baud-rate 493
domain-name 494
hostname 495
led locator 495
mtrace 496

power consumption-average-period 498
show bluetooth 498
show boot-history 500
show capacities 503
show capacities-status 504
show console 505
show core-dump 506
show deprecated commands 508
show domain-name 509
show environment fan 510
show environment led 511
show environment power-consumption 512
show environment power-redundancy 515
show environment power-supply 515
show environment temperature 517
show events 518
show hostname 521
show images 522
show ip errors 523
show module 525
show running-config 527
show running-config current-context 530
show startup-config 531
show system 533
show system resource-utilization 535
show tech 537
show usb 539
show usb file-system 540
show version 541
system resource-utilization poll-interval 542
top cpu 543
top memory 543
usb 544
usb mount | unmount 545

Support and Other Resources 547

Accessing HPE Aruba Networking Support 547
Accessing Updates 548
Warranty Information 548
Regulatory Information 548
Documentation Feedback 548

Chapter 1
About this document

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

Applicable products

This document applies to the following products:

- HPE Aruba Networking 8100 Switch Series (R9W94A, R9W95A, R9W96A, R9W97A)
- HPE Aruba Networking 8320 Switch Series (JL479A, JL579A, JL581A)
- HPE Aruba Networking 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- HPE Aruba Networking 8325H Switch Series (S4B20A, S4B21A, S4B22A, S4B23A, S2T42A, S2T46A, S2T47A, S2T48A)
- HPE Aruba Networking 8325P Switch Series (S0G12A, S4A48A)
- HPE Aruba Networking 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A, JL700C, JL701C, JL702C, JL703C, JL706C, JL707C, JL708C, JL709C, JL710C, JL711C, JL704C, JL705C, JL719C, JL718C, JL717C, JL720C, JL722C, JL721C)
- HPE Aruba Networking 9300 Switch Series (R9A29A, R9A30A, R8Z96A, S0F81A, S0F82A, S0F83A)
- HPE Aruba Networking 9300S Switch Series (S0F81A, S0F82A, S0F83A, S0F84A, S0F85A, S0F86A, S0F88A, S0F95A, S0F96A)
- HPE Aruba Networking 10000 Switch Series (R8P13A, R8P14A)

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>	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

Convention	Usage
■ *example-text* ■ *example-text*	are enclosed in angle brackets (**< >**). Substitute the text—including the enclosing angle brackets—with an actual value. ■ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
|	Vertical bar. A logical **OR** that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[ ]	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

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

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

Understanding the CLI prompts

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

```
switch>
```

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

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

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

Indicates the configuration context for a feature. For example:

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

Identifies the **interface** context.

Variable information in CLI prompts

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

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

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

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

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

Identifying switch ports and interfaces

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

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

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

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

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

Chapter 2
About AOS-CX

AOS-CX is a new, modern, fully programmable operating system built using a database-centric design that ensures higher availability and dynamic software process changes for reduced downtime. In addition to robust hardware reliability, the AOS-CX operating system includes additional software elements not available with traditional systems, including:

- Automated visibility to help IT organizations scale: The HPE Aruba Networking Network Analytics Engine allows IT to monitor and troubleshoot network, system, application, and security-related issues easily through simple scripts. This engine comes with a built-in time series database that enables customers and developers to create software modules that allow historical troubleshooting, as well as analysis of historical trends to predict and avoid future problems due to scale, security, and performance bottlenecks.
- Programmability simplified: A switch that is running the AOS-CX operating system is fully programmable with a built-in Python interpreter as well as REST-based APIs, allowing easy integration with other devices both on premise and in the cloud. This programmability accelerates IT organization understanding of and response to network issues. The database holds all aspects of the configuration, statistics, and status information in a highly structured and fully defined form.
- Faster resolution with network insights: With legacy switches, IT organizations must troubleshoot problems after the fact, using traditional tools like CLI and SNMP, augmented by separate, expensive monitoring, analytics, and troubleshooting solutions. These capabilities are built in to the AOS-CX operating system and are extensible.
- High availability: For switches that support active and standby management modules, the AOS-CX database can synchronize data between active and standby modules and maintain current configuration and state information during a failover to the standby management module.
- Ease of roll-back to previous configurations: The built-in database acts as a network record, enabling support for multiple configuration checkpoints and the ability to roll back to a previous configuration checkpoint.

AOS-CX system databases

The AOS-CX operating system is a modular, database-centric operating system. Every aspect of the switch configuration and state information is modeled in the AOS-CX switch configuration and state database, including the following:

- Configuration information
- Status of all features
- Statistics

The AOS-CX operating system also includes a time series database, which acts as a built-in network record. The time series database makes the data seamlessly available to HPE Aruba Networking Network Analytics Engine agents that use rules that evaluate network conditions over time. Time-series data about the resources monitored by agents are automatically collected and presented in graphs in the switch Web UI.

Network Analytics Engine introduction

The HPE Aruba Networking Network Analytics Engine is a first-of-its-kind built-in framework for network assurance and remediation. Combining the full automation and deep visibility capabilities of the AOS-CX operating system, this unique framework enables monitoring, collecting network data, evaluating conditions, and taking corrective actions through simple scripting agents.

This engine is integrated with the AOS-CX system configuration and time series databases, enabling you to examine historical trends and predict future problems due to scale, security, and performance bottlenecks. With that information, you can create software modules that automatically detect such issues and take appropriate actions.

With the faster network insights and automation provided by the HPE Aruba Networking Network Analytics Engine, you can reduce the time spent on manual tasks and address current and future demands driven by Mobility and IoT.

AOS-CX CLI

The AOS-CX CLI is an industry standard text-based command-line interface with hierarchical structure designed to reduce training time and increase productivity in multivendor installations.

The CLI gives you access to the full set of commands for the switch while providing the same password protection that is used in the Web UI. You can use the CLI to configure, manage, and monitor devices running the AOS-CX operating system.

HPE Aruba Networking Installer mobile app

The HPE Aruba Networking Installer mobile app enables you to use a mobile device to configure or access a supported AOS-CX switch. You can connect to the switch through Bluetooth or Wi-Fi.

You can use this application to do the following:

- Connect to the switch for the first time and configure basic operational settings—all without requiring you to connect a terminal emulator to the console port.
- View and change the configuration of individual switch features or settings.
- Manage the running configuration and startup configuration of the switch, including the following:
  - Transferring files between the switch and your mobile device
  - Sharing configuration files from your mobile device
  - Copying the running configuration to the startup configuration
- Access the switch CLI.

Refer to the HPE Aruba Networking Installer mobile app datasheet for more information.

HPE Aruba Networking NetEdit

HPE Aruba Networking NetEdit enables the automation of multidevice configuration change workflows without the overhead of programming.

The key capabilities of NetEdit include the following:

- Intelligent configuration with validation for consistency and compliance
- Time savings by simultaneously viewing and editing multiple configurations
- Customized validation tests for corporate compliance and network design

- Automated large-scale configuration deployment without programming
- Ability to track changes to hardware, software, and configurations (whether made through NetEdit or directly on the switch) with automated versioning

For more information about HPE Aruba Networking NetEdit, search for NetEdit at the following website:

www.hpe.com/support/hpesc

Ansible modules

Ansible is an open-source IT automation platform.

HPE Aruba Networking publishes a set of Ansible configuration management modules designed for switches running AOS-CX software. The modules are available from the following places:

- The **arubanetworks.aoscx_role** role in the Ansible Galaxy at: https://galaxy.ansible.com/arubanetworks/aoscx_role
- The **aoscx-ansible-role** at the following GitHub repository: https://github.com/aruba/aoscx-ansible-role

AOS-CX Web UI

The Web UI gives you quick and easy visibility into what is happening on your switch, providing faster problem detection, diagnosis, and resolution. The Web UI provides dashboards and views to monitor the status of the switch, including easy to read indicators for: power supply, temperature, fans, CPU use, memory use, log entries, system information, firmware, interfaces, VLANs, and LAGs. In addition, you use the Web UI to access the Network Analytics Engine, run certain diagnostics, and modify some aspects of the switch configuration.

AOS-CX REST API

Switches running the AOS-CX software are fully programmable with a REST (REpresentational State Transfer) API, allowing easy integration with other devices both on premises and in the cloud. This programmability—combined with the HPE Aruba Networking Network Analytics Engine—accelerates network administrator understanding of and response to network issues.

The AOS-CX REST API enables programmatic access to the AOS-CX configuration and state database at the heart of the switch. By using a structured model, changes to the content and formatting of the CLI output do not affect the programs you write. And because the configuration is stored in a structured database instead of a text file, rolling back changes is easier than ever, thus dramatically reducing a risk of downtime and performance issues.

The AOS-CX REST API is a web service that performs operations on switch resources using HTTPS **POST**, **GET**, **PUT**, **DELETE**, and **PATCH** methods.

A switch resource is indicated by its Uniform Resource Identifier (URI). A URI can be made up of several components, including the host name or IP address, port number, the path, and an optional query string. The AOS-CX operating system includes the AOS-CX REST API Reference, which is a web interface based on the Swagger UI. The AOS-CX REST API Reference provides the reference documentation for the REST API, including resources URIs, models, methods, and errors. The AOS-CX REST API Reference shows most of the supported read and write methods for all switch resources.

In-band and out-of-band management

Management communications with a managed switch can be either of the following:

In band

In-band management communications occur through ports on the line modules of the switch, using common communications protocols such as SSH and SNMP.

When you use an in-band management connection, management traffic from that connection uses the same network infrastructure as user data. User data uses the `data plane`, which is responsible for moving data from source to destination. Management traffic that uses the data plane is more likely to be affected by traffic congestion and other issues affecting the user network.

Out of band

OOBM (out-of-band management) communications occur through a dedicated serial or USB console port or though a dedicated networked management port.

OOBM operates on a `management plane` that is separate from the `data plane` used by data traffic on the switch and by in-band management traffic. That separation means that OOBM can continue to function even during periods of traffic congestion, equipment malfunction, or attacks on the network. In addition, it can provide improved switch security: a properly configured switch can limit management access to the management port only, preventing malicious attempts to gain access through the data ports.

Networked OOBM typically occurs on a management network that connects multiple switches. It has the added advantage that it can be done from a central location and does not require an individual physical cable from the management station to the console port of each switch.

SNMP-based management support

The AOS-CX operating system provides SNMP read access to the switch. SNMP support includes support of industry-standard MIB (Management Information Base) plus private extensions, including SNMP events, alarms, history, statistics groups, and a private alarm extension group. SNMP access is disabled by default.

User accounts

To view or change configuration settings on the switch, users must log in with a valid account. Authentication of user accounts can be performed locally on the switch, or by using the services of an external TACACS+ or RADIUS server.

Two types of user accounts are supported:

- Operators: Operators can view configuration settings, but cannot change them. No operator accounts are created by default.
- Administrators: Administrators can view and change configuration settings. A default locally stored administrator account is created with username set to **admin** and no password. You set the administrator account password as part of the initial configuration procedure for the switch.

Chapter 3
Initial Configuration

Perform the initial configuration of a factory default switch using one of the following methods:

- Load a switch configuration using zero-touch provisioning (ZTP). When ZTP is used, the configuration is loaded from a server automatically when the switch booted from the factory default configuration.
- Connect to the switch wirelessly with a mobile device through Bluetooth, and use the HPE Aruba Networking Installer Mobile App to deploy an initial configuration from a provided template. The template you choose during the deployment process determines how the management interface is configured. Optionally, as the final deployment step, you can select to import the switch into NetEdit through a WiFI connection to the NetEdit server.

Alternatively, you can use the HPE Aruba Networking Installer Mobile App to manually configure switch settings and features for a subset of the features you can configure using the CLI. You can also access the CLI through the mobile application.

- 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. Configure switch settings and features by executing CLI commands.
- Connect a computer running terminal emulation software to the console port on the switch. Configure switch settings and features by executing CLI commands.

Reserved ports or ports used by other applications/services with in the system are not recommended to be used for other services. When two services use the same port there is chance of unexpected behaviors from these services. Best practices is to use unique port for each service across system.

Initial configuration using ZTP

Zero Touch Provisioning (ZTP) configures a switch automatically from a remote server.

Prerequisites

- The switch must be in the factory default configuration.

Do not change the configuration of the switch from its factory default configuration in any way, including by setting the administrator password.

- Your network administrator or installation site coordinator must provide a Category 6 (Cat6) cable connected to the network that provides access to the servers used for Zero Touch Provisioning (ZTP) operations.

Procedure

1. Connect the network cable to the out-of-band management port on the switch.

   See the *Installation Guide* for switch to determine the location of the switch ports.
2. If the switch is powered on, power off the switch.

3. Power on the switch. During the ZTP operation, the switch might reboot if a new firmware image is being installed. ZTP goes to "Failed" state if the switch receives DHCP IP for vlan1 and does not receive any ZTP options within 60 seconds.

Initial configuration using the HPE Aruba Networking Installer mobile app

This procedure describes how to use your mobile device to connect to the Bluetooth interface of the switch to connect to the switch for the first time so that you can configure basic operational settings using the HPE Aruba Networking Installer mobile app.

Prerequisites

- You have obtained the USB Bluetooth adapter that was shipped with the switch. Information about the make and model of the supported adapter is included in the information about the HPE Aruba Networking Installer Mobile App in the Apple Store or Google Play.
- The HPE Aruba Networking Installer Mobile App must be installed on your mobile device.
- Bluetooth must be enabled on your mobile device.
- Your mobile device must be within the communication range of the Bluetooth adapter.
- If you are planning to import the switch into NetEdit, your mobile device must be able to use a Wi-Fi connection—not Bluetooth—to access the NetEdit server.

If your mobile device does not support simultaneous Bluetooth and Wi-Fi connections, you must use the NetEdit interface to import the switch at a later time. You can use the **Devices** tab to display the IP address of the switches you configured using your mobile device.

- The switch must be installed and powered on, with the network operating system boot sequence complete.

For information about installing and powering on the switch, see the *Installation Guide* for the switch.

Because you are using this mobile application to configure the switch through the Bluetooth interface, it is not necessary to connect a console to the switch.

- Bluetooth and USB must be enabled on the switch. On switches shipped from the factory, Bluetooth and USB are enabled by default.

Procedure

1. Install the USB Bluetooth adapter in the USB port of the switch.

   For switches that have multiple management modules, you must install the USB Bluetooth adapter in the USB port of the active management module. Typically, the active management module is the module in slot 5.

   Switches shipped from the factory have both USB and Bluetooth enabled by default.

   For information about the location of the USB port on the switch, see the *Installation Guide* for the switch.
2. Use the Bluetooth settings on your mobile device to pair and connect the switch to your mobile device.

   If you are in range of multiple Bluetooth devices, more than one device is displayed on the list of available devices. Switches running the AOS-CX operating system are displayed in the following format:

   ```
   Switch_model - Serial_number
   ```

For example: `8325-987654X1234567` or `8320-AB12CDE123`

A switch supports one active Bluetooth connection at a time.

On some Android devices, you might need to change the settings of the paired device to specify that it be used for Internet access.

3. Open the HPE Aruba Networking Installer mobile app on your mobile device.

The application attempts to connect to the switch using the switch Bluetooth IP address and the default switch login credentials. The **Home** screen of the application shows the status of the connection to the switch:

- If the login attempt was successful, the Bluetooth icon is displayed and the status message shows the Bluetooth IP address of the switch. In addition, the connection graphic is green. You can continue to the next step.
- If the login attempt was not successful, but a response was received, the Bluetooth icon is displayed, but the status message is: **Login Required**. You can continue to the next step. When you tap one of the tiles, you will be prompted for login credentials.
- If the login attempt did not receive a response, the Bluetooth icon is not displayed, and the status message is: **No Connection**.

4. Create the initial switch configuration:
   - You can deploy an initial configuration to the switch. Through this process, you supply the information required by a configuration template that you choose from a list of templates provided by the application. Then you deploy the configuration to the switch and, optionally, import the switch into NetEdit.

When you deploy a switch configuration, it becomes the running configuration, replacing the entire existing configuration of the switch. All changes previously made to the factory default configuration are overwritten.
If you plan to both deploy a switch configuration and customize the configuration of switch features, deploy the initial configuration first.

To deploy an initial switch configuration, tap: **Initial Config** and follow the instructions in the application.

- Alternatively, you can complete the initial configuration of the switch by tapping **Modify Config** and then selecting the features and settings to configure.
- You can also use the **Modify Config** feature to configure some switch features after the initial configuration is complete. For more information about what you can configure using the HPE Aruba Networking Installer mobile app, see the online help for the application.

Troubleshooting Bluetooth connections

Bluetooth connection IP addresses

The Bluetooth connection uses IP addresses in the 192.168.99.0/24 subnet.

Switch

192.168.99.1

Mobile device

192.168.99.10

Bluetooth is connected but the switch is not reachable

Symptom

The mobile device settings indicate that the device is connected to the switch through Bluetooth. However, the mobile application indicates that the switch is not reachable.

Solution 1

Cause

The mobile device is paired with a different nearby switch.

Action

1. Verify the model number and serial number of the switch to which you are attempting to connect.
2. Use the Bluetooth settings on your mobile device to pair and connect the switch to your mobile device.

If you are in range of multiple Bluetooth devices, more than one device is displayed on the list of available devices. Switches running the AOS-CX operating system are displayed in the following format: *`Switch_model-Serial_number`*

For example: `8325-987654X1234567` or `8320-AB12CDE123`

A switch supports one active Bluetooth connection at a time.

On some Android devices, you might need to change the settings of the paired device to specify that it be used for Internet access.

Solution 2

Cause

The mobile device is connected to a different network—such as through a Wi-Fi connection—that conflicts with the subnet used for the switch Bluetooth connection.

Action

Disconnect the mobile device from the network that is using the conflicting subnet.

For example, use the mobile device settings to turn off or disable Wi-Fi. If you choose to disable Wi-Fi on the mobile device, and you are not able to access cellular service, you will not be able to connect to the NetEdit server to import the switch, but you can still deploy a switch configuration.

Bluetooth is not connected

Symptom

Your mobile device cannot establish a Bluetooth connection to the switch.

Solution 1

Cause

Bluetooth is not enabled on your mobile device.

Action

- Use your mobile device settings application to enable Bluetooth.
- Use the Bluetooth settings on your mobile device to pair and connect the switch to your mobile device.

If you are in range of multiple Bluetooth devices, more than one device is displayed on the list of available devices. Switches running the AOS-CX operating system are displayed in the following format:
Switch_model-Serial_number

For example: **8325-987654X1234567** or **8320-AB12CDE123**

A switch supports one active Bluetooth connection at a time.

On some Android devices, you might need to change the settings of the paired device to specify that it be used for Internet access.

Solution 2

Cause

Your mobile device is not within the broadcast range of the Bluetooth adapter.

Action

Move closer to the switch.

Devices can communicate through Bluetooth when they are close, typically within a few feet of each other.

Solution 3

Cause

Your mobile device is not paired with the switch.

Action

1. Use your mobile device settings application to enable Bluetooth.
2. Use the Bluetooth settings on your mobile device to pair and connect the switch to your mobile device.

   If you are in range of multiple Bluetooth devices, more than one device is displayed on the list of available devices. Switches running the AOS-CX operating system are displayed in the following format:
   Switch_model-Serial_number

   For example: **8325-987654X1234567** or **8320-AB12CDE123**

   A switch supports one active Bluetooth connection at a time.
3. On some Android devices, you might need to change the settings of the paired device to specify that it be used for Internet access.

Solution 4

Cause

Bluetooth is not enabled on the switch.

New switches are shipped from the factory with the USB port and Bluetooth enabled. However, an installed switch might have been configured to disable Bluetooth or disable the USB port, which the USB Bluetooth adapter uses.

Action

Use a different CLI connection to enable Bluetooth on the switch.

- Use the **show bluetooth** CLI command to show the Bluetooth configuration and the status of the Bluetooth adapter.
- To enable the USB port, enter the CLI command: **usb**

- An inserted USB drive must be mounted each time the switch boots or fails over to a different management module. To mount the drive, enter the CLI command: **usb mount**
- To enable Bluetooth, enter the CLI command: **bluetooth enable**

Solution 5

Cause

Another mobile device has already connected to the switch through Bluetooth. This cause is likely if your device is repeatedly disconnected within 1-2 seconds of establishing a connection.

Action

1. Use a different CLI connection to see if there is another device connected:

   Use the **show bluetooth** CLI command to show the Bluetooth configuration and the status of the Bluetooth adapter.
2. Either disconnect the other device or use that device to communicate with the switch.

   A switch can use Bluetooth to connect to one mobile device at a time.

Solution 6

Cause

The switch has been restarted since the mobile device was last paired with the switch, and the device is having difficulty establishing the Bluetooth connection.

Action

1. Use the Bluetooth mobile device settings to forget the switch device.
2. Use your mobile device settings application to disable Bluetooth.
   Use your mobile device settings application to enable Bluetooth.

   If you are in range of multiple Bluetooth devices, more than one device is displayed on the list of available devices. Switches running the AOS-CX operating system are displayed in the following format:
   Switch_model-Serial_number

   For example: **8325-987654X1234567** or **8320-AB12CDE123**

   A switch supports one active Bluetooth connection at a time.

   On some Android devices, you might need to change the settings of the paired device to specify that it be used for Internet access.

Solution 7

Cause

The USB Bluetooth adapter is not installed in the switch.

If the switch has multiple management modules, the USB Bluetooth adapter might be installed in the management module that is not the active management module.

Action

Install the USB Bluetooth adapter in the USB port of the switch.

For switches that have multiple management modules, you must install the USB Bluetooth adapter in the USB port of the active management module. Typically, for new switches, the active management module is the module in slot 5 (HPE Aruba Networking 8400 switches) or slot 1 (HPE Aruba Networking 6400 switches).

For information about the location of the USB port on the switch, see the *Installation Guide* for the switch.

Solution 8

Cause

A problem occurred with the Bluetooth feature on the switch. For example, the software daemon was stopped and then restarted.

Action

1. Use a different connection to the switch CLI to disable and then enable Bluetooth.

   ```
   switch(config)# bluetooth disable
   switch(config)# bluetooth enable
   ```

2. Use the Bluetooth mobile device settings to forget the switch device.
3. Use your mobile device settings application to disable Bluetooth.
4. Use your mobile device settings application to enable Bluetooth.
5. Use your mobile device settings application to enable Bluetooth.

   If you are in range of multiple Bluetooth devices, more than one device is displayed on the list of available devices. Switches running the AOS-CX operating system are displayed in the following format:
   Switch_model-Serial_number

   For example: **8325-987654X1234567** or **8320-AB12CDE123**

   A switch supports one active Bluetooth connection at a time.

   On some Android devices, you might need to change the settings of the paired device to specify that it be used for Internet access.

Solution 9

Cause

A switch that is member of a stack (but is not the conductor switch), has a USB Bluetooth adapter installed, but mobile application has lost contact with that switch.

Action

Remove and then reinstall the USB Bluetooth adapter.

Do not remove the USB Bluetooth adapter from the conductor switch.

Initial configuration using the CLI

This procedure describes how to connect to the switch for the first time and configure basic operational settings using the CLI. In this procedure, you use a computer to connect to the switch using the either the console port or management port.

Procedure

1. Connect to the console port or the management port.
2. Log into the switch for the first time.
3. Configure switch time using the NTP client.

Connecting to the console port

Prerequisites

- A switch installed as described in its hardware installation guide.
- A computer with terminal emulation software.
- A JL448A HPE Aruba Networking X2 C2 RJ45 to DB9 console cable.

Procedure

1. Connect the console port on the switch to the serial port on the computer using a console cable.
2. Start the terminal emulation software on the computer and configure a new serial session with the following settings:
   - Speed: 115200 bps
   - Data bits: 8
   - Stop bits: 1
   - Parity: None
   - Flow control: None
3. Start the terminal emulation session.
4. Press **Enter** once. If the connection is successful, you are prompted to log in.

Optional console port speed setting

If desired, the console port speed can be set with the **console baud-rate** command. For example, 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
```

Showing the console port current speed:

```
switch# show console
Baud Rate: 9600
```

For details on the **console baud-rate** and **show console** commands, see Switch system and hardware commands.

Connecting to the management port

Prerequisites

- Two Ethernet cables
- SSH client software

Procedure

1. By default, the management interface is set to automatically obtain an IP address from a DHCP server, and SSH support is enabled. If there is no DHCP server on your network, you must configure a static address on the management interface:

a. Connect to the console port
b. Configure the management interface.

2. Use an Ethernet cable to connect the management port to your network.
3. Use an Ethernet cable to connect your computer to the same network.
4. Start your SSH client software and configure a new session using the address assigned to the management interface. (If the management interface is set to operate as a DHCP client, retrieve the IP address assigned to the management interface from your DHCP server.)
5. Start the session. If the connection is successful, you are prompted to log in.

Logging into the switch for the first time

The first time you log in to the switch you must use the default administrator account. This account has no password, so you will be prompted on login to define one to safeguard the switch.

Procedure

1. When prompted to log in, specify **admin**. When prompted for the password, press **ENTER**. (By default, no password is defined.)

   For example:

   ```
   switch login: admin
   password:
   ```

2. Define a password for the **admin** account. The password can contain up to 32 alphanumeric characters in the range ASCII 32 to 127, which includes special characters such as asterisk (*), ampersand (&), exclamation point (!), dash (-), underscore (_), and question mark (?).

   For example:

   ```
   Please configure the 'admin' user account password.
   Enter new password: *******
   Confirm new password: *******
   switch#
   ```

3. You are placed into the manager command context, which is identified by the prompt: `switch#`, where `switch` is the model number of the switch. Enter the command `config` to change to the global configuration context `config`.

   For example:

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

Setting switch time using the NTP client

Prerequisites

- The IP address or domain name of an NTP server.
- If the NTP server uses authentication, obtain the password required to communicate with the NTP server.

Procedure

1. If the NTP server requires authentication, define the authentication key for the NTP client with the command **ntp authentication**.
2. Configure an NTP server with the command **ntp server**. When configuring a time backward more than five minutes on the HPE Aruba Networking 8320, 8325, or 9300 Switch Series, a reboot is recommended to avoid unusual switch behavior.
3. By default, NTP traffic is sent on the default VRF. If you want to send NTP traffic on the management VRF, use the command **ntp vrf**.
4. Review your NTP configuration settings with the commands **show ntp servers** and `show ntp status`.
5. See the current switch time, date, and time zone with the command **show clock**.

Example

This example creates the following configuration:

- Defines the authentication key **1** with the password **myPassword**.
- Defines the NTP server **my-ntp.mydomain.com** and makes it the preferred server.
- Sets the switch to use the management VRF (**mgmt**) for all NTP traffic.

```
switch(config)# ntp authentication-key 1 md5 myPassword
switch(config)# ntp server my-ntp.mydomain.com key 10 prefer
switch(config)# ntp vrf mgmt
```

Configuring banners

1. Configure the banner that is displayed when a user connects to a management interface. Use the command `banner motd`. For example:

```
switch(config)# banner motd ^
Enter a new banner. Terminate the banner with the delimiter you have chosen.
>> 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.^
Banner updated successfully!
```

2. Configure the banner that is displayed after a user is authenticated. Use the command `banner exec`. For example:

```
switch(config)# banner exec &
Enter a new banner. Terminate the banner with the delimiter you have chosen.
>> This is an example of a different banner text. This time
>> the banner entered will be displayed after a user has
>> authenticated.
>>
```

```
>> & This text will not be included because it comes after the '&'
Banner updated successfully!
```

Configuring in-band management on a data port

Prerequisites

- A connection to the CLI via either the console port or the management port
- Ethernet cable

Procedure

1. Use an Ethernet cable to connect a data port to your network.
2. Configure a layer 3 interface on the data port.
3. Enable SSH support on the interface (on the default VRF) with the command `ssh server vrf default`.

   For example:
   ```
   switch# config
   switch(config)# ssh server vrf default
   ```
4. Enable the Web UI on the interface (on the default VRF) with the command `https-server vrf default`.

   For example:
   ```
   switch(config)# https-server vrf default
   ```

Using the Web UI

The Web UI is disabled by default. Follow these steps to enable it on the management port and log in. The Web UI is enabled by default on the default VRF.

Prerequisites

- A connection to the switch CLI.

Procedure

1. Log in to the CLI.
2. Switch to `config` context and enable the Web UI on the management port VRF with the command `https-server vrf mgmt`.

   For example:

   ```
   switch# config
   switch(config)# https-server vrf mgmt
   ```
3. Start your web browser and enter the IP address of the management port in the address bar,

   For example: **https://192.168.1.1**
4. The Web UI starts and you are prompted to log in.

Configuring the management interface

Prerequisites

A connection to the console port.

Procedure

1. Switch to the management interface context with the command `interface mgmt`.
2. By default, the management interface on the management port is enabled. If it was disabled, re-enable it with the command `no shutdown`.
3. Use the command `ip dhcp` to configure the management interface to automatically obtain an address from a DHCP server on the network (factory default setting). Or, assign a static IPv4 or IPv6 address, default gateway, and DNS server with the commands `ip address`, `ipv6 address`, `ip static`, `default-gateway`, and `nameserver`.
4. SSH is enabled by default on the management VRF. If disabled, enable SSH with the command `ssh server vrf mgmt`.

Examples

This example enables the management interface with dynamic addressing using DHCP:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# no shutdown
switch(config-if-mgmt)# ip dhcp
```

This example enables the management interface with static addressing creating the following configuration:

- Sets a static IPv4 address of **198.168.100.10** with a mask of **24** bits.
- Sets the default gateway to **198.168.100.200**.
- Sets the DNS server to **198.168.100.201**.

```
switch(config)# interface mgmt
switch(config-if-mgmt)# no shutdown
switch(config-if-mgmt)# ip static 198.168.100.10/24
switch(config-if-mgmt)# default-gateway 198.168.100.200
switch(config-if-mgmt)# nameserver 198.168.100.201
```

IP prefix priority

IP prefix priority applies to the 8360 Switch Series.

IP prefix priority configuration is used to optimize route lookup based on the IP address prefix length, sometimes known as the IP subnet mask length. Switch models supporting IP prefix priority configuration have six lookup tables with the first five being configurable for specific prefix lengths and the last one being used for all other prefix lengths.

The default configuration of the five exact IP prefix tables use common lengths typical to many networks. For sites that make extensive use of atypical IP prefix lengths (lengths that differ from the defaults), the exact prefix tables can be customized by configuring IP prefix priority. Doing so avoids over filling the “other” table and keeps as many routes as possible in the fast-path.

Commands **`show ip prefix-priority`** and **`show ipv6 prefix-priority`** show the default, current, and any pending IP prefix priority configuration for a switch.

See also IP Prefix priority commands.

System profiles and configurable IP prefix priority

System profiles set the overall capabilities and capacities of the switch (including IP prefix partitions), based on the selected profile used at boot time. Only certain profiles support configurable IP prefix priority.

To use configurable IP prefix priority, the switch must be booted into a capable profile. If a switch is booted into a profile that does not support configurable IP prefix priority, a warning is displayed before the reboot, and upon reboot, the default IP prefix tables are used and any configured IP prefix priority is discarded.

See also Selecting the system profile.

IP prefix priority defaults

This default IP prefix priority information only applies to system profiles specifically named here. Any profile unnamed here does not support configurable IP prefix priority.

8360 Switch Series, profile: **Core-Spine** (five prefix values required):

- **IPv4**: 24, 23, 22, 21, 20
- **IPv6**: 64, 48, 44, 36, 32

IP Prefix priority commands

ip prefix-priority

```
ip prefix-priority <PREFIX-LENGTHS>
no ip prefix-priority [<PREFIX-LENGTHS>>]
```

Description

Configures custom IPv4 route prefix lengths for the exact prefix match tables of the switch. The switch must be rebooted to apply the change.

Following the reboot, IPv4 prefix priorities will remain in a pending state until at least one route is learned. A connected route counts so this can be as simple as having an L3 interface with an IP address in the up state.

The no form of this command resets the prefix lengths to their default

Parameter	Description
<PREFIX-LENGTHS>>	Specifies a space-separated list of exactly five prefix lengths, in descending order. Range: 8 to 31.

Examples

Configuring custom IPv4 route prefix lengths:

```
switch(config)# ip prefix-priority 29 28 27 24 16
Save this config and reboot the switch for the changes to take effect
...
```

Resetting IPv4 route prefix lengths to their default:

```
switch(config)# no ip prefix-priority
Save this config and reboot the switch for the changes to take effect
...
```

Attempting to configure custom IPv4 route prefix lengths with some lengths not in descending order:

```
switch(config)# ip prefix-priority 28 29 27 23 16
Prefix lengths must be specified in descending order
```

Attempting to configure eight prefix lengths:

```
switch(config)# ip prefix-priority 29 28 27 24 23 16 12 8
Invalid input: 16
```

Attempting to configure three prefix lengths:

```
switch(config)# ip prefix-priority 29 28 27
% Command incomplete.
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	config	Administrators or local user group members with execution rights for this command.

ipv6 prefix-priority

```
ipv6 prefix-priority <PREFIX-LENGTHS>
no ipv6 prefix-priority [<PREFIX-LENGTHS>>]
```

Description

Configures custom IPv6 route prefix lengths for the exact prefix match tables of the switch. The switch must be rebooted to apply the change.

Following the reboot, IPv6 prefix priorities will remain in a pending state until at least one route is learned. A connected route counts so this can be as simple as having an L3 interface with an IP address in the up state.

The no form of this command resets the prefix lengths to their default

Parameter	Description
<PREFIX-LENGTHS>>	Specifies a space-separated list of exactly five prefix lengths, in descending order. Range: 8 to 64.

Examples

Configuring custom IPv6 route prefix lengths:

```
switch(config)# ipv6 prefix-priority 64 63 62 32 28
Save this config and reboot the switch for the changes to take effect
...
```

Resetting IPv6 route prefix lengths to their default:

```
switch(config)# no ipv6 prefix-priority
Save this config and reboot the switch for the changes to take effect
...
```

Attempting to configure custom IPv6 route prefix lengths with some lengths not in descending order:

```
switch(config)# ipv6 prefix-priority 64 62 63 31 32
Prefix lengths must be specified in descending order
```

Attempting to configure eight prefix lengths:

```
switch(config)# ipv6 prefix-priority 64 63 62 32 31 28 24 23
Invalid input: 28
```

Attempting to configure three prefix lengths:

```
switch(config)# ipv6 prefix-priority 64 63 31
% Command incomplete.
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	`config`	Administrators or local user group members with execution rights for this command.

show ip prefix-priority

```
show ip prefix-priority
```

Description

Shows the configuration, status, and defaults of the IPv4 route prefix lengths for the exact prefix match tables of the switch.

Examples

Showing configured IPv4 route prefix lengths that are pending until the switch is rebooted and at least one route is learned:

```
switch# show ip prefix-priority

 IP Exact-Prefix Table Information

 Configuration Status: Ready to apply on next reboot

          Default   Current   Pending
  Table    Length    Length    Length
  ----------------------------------
  1            24        24        29*
  2            23        23        28*
  3            22        22        27*
  4            21        21        24*
  5            20        20        23*

  * Pending values will be applied on the next reboot
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators 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 prefix-priority

```
show ipv6 prefix-priority
```

Description

Shows the configuration, status, and defaults of the IPv6 route prefix lengths for the exact prefix match tables of the switch.

Examples

Showing configured IPv6 route prefix lengths that are pending until the switch is rebooted and at least one route is learned:

```
switch# show ipv6 prefix-priority

 IPv6 Exact-Prefix Table Information

 Configuration Status: Ready to apply on next reboot

          Default   Current   Pending
  Table    Length    Length    Length
  ------------------------------------
  1            64        64        64
  2            48        48        63*
  3            44        44        62*
  4            36        36        32*
  5            32        32        31*

  * Pending values will be applied on the next reboot
```

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Selecting the system profile

System profiles set the overall capabilities and capacities of the switch, based on the selected profile used at boot time. System profiles set capacities such as that of the hardware forwarding table.

System profiles provide you with the flexibility to configure switches based on their location in the network (for example, core, spine, leaf). When a switch boots without a profile specifically configured, it boots with the default profile. When a switch is configured with a non-default profile, the switch requires a reboot for the profile to be applied.

Command **`show profiles available`** shows all profiles available on a particular switch.

See also System profile commands.

Procedure

1. Set the system profile with the command `profile`.
2. Reboot the switch for the profile change to take effect with the command `boot system`.

Examples

(8320, 8325, 9300, 10000) Selecting the **`l3-agg`** profile and then rebooting the system:

```
switch(config)# profile l3-agg
switch(config)# exit
switch# boot system
...
```

(8320, 8325, 9300, 10000) Selecting the **Spine** profile and then rebooting the system:

```
switch(config)# profile Spine
switch(config)# exit
switch# boot system
...
```

(8360) Selecting the **Core-Spine** profile and then rebooting the system:

```
switch(config)# profile Core-Spine
switch(config)# exit
switch# boot system
...
```

System profile commands

profile

```
profile <PROFILE-NAME>
no profile [<PROFILE-NAME>]
```

Description

Selects the system profile. System profiles set the overall capabilities and capacities of the switch based on the selected profile used at boot time. Switch profiles set capacities such as that of the hardware forwarding table. Use command show profiles available to show the details of each available profile.

When a switch is configured with a non-default profile, the switch requires a reboot for the profile to be applied. You are prompted for the reboot.

The **no** form of this command resets the specified profile to its defaults.

Usage

Profiles supported on 8320, 8325/8325H/8325P and 10000 Switch Series:

Profile names	Description
L3-agg	Optimizes for layer 3 forwarding with more table space allocated to host(ARP/ND) entries.
L3-core	(The default on the 8320 Switch Series.) Optimize for layer 3 forwarding with more table space allocated to route entries.
Leaf	(The default on the 8325/8325H/8325P, and 10000 Switch Series.) Optimizes for layer 2 forwarding with more table space allocated to overlay host entries (VXLAN).

Profile names	Description
spine	Optimizes for layer 3 forwarding with more table space allocated to route entries.

Profiles supported on 9300 and 9300S Switch series:

Profile names	Description
Leaf	Optimizes for layer 2 forwarding with more table space allocated to overlay host entries (VXLAN).
spine	Optimizes for layer 3 forwarding with more table space allocated to route entries.
DC-Optimized-Spine	Spine profile optimized for datacenter deployments. The DC-Optimized-Spine profile does not support IP tunnels, including 6in4 tunnels, 6in6 tunnels, and GRE tunnels.
DC-Optimized-Leaf	(The default on the 9300/9300S Switch Series.) Leaf profile optimized for datacenter deployments. The DC-Optimized-leaf profile does not support IP tunnels, including 6-in-4 tunnels, 6-in-6 tunnels, and GRE tunnels.

Profiles supported on 8360 Switch Series:

Profile names	Description
Aggregation-Leaf	(The default.) Optimizes for aggregation leaf.
Core-Spine	Optimizes for core spine.
Leaf-Extended	Optimizes for leaf extended.

Examples

(8320, 8325, 9300, 10000) Selecting the L3-agg profile and then rebooting the system:

```
switch(config)# profile l3-agg
switch(config)# exit
switch# boot system
...
```

(8320, 8325, 9300, 10000) Selecting the Spine profile and then rebooting the system:

```
switch(config)# profile Spine
switch(config)# exit
switch# boot system
...
```

(8360) Selecting the Core-Spine profile and then rebooting the system:

```
switch(config)# profile Core-Spine
switch(config)# exit
switch# boot system
...
```

Command History

Release	Modification
10.09	Command Introduced on the 10000.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8320 8325 8325H 8325P 8360 9300 9300S 10000	config	Administrators or local user group members with execution rights for this command.

show profiles available

```
show profiles available
```

Description

Shows all system profile names available and profile details.

Examples

Showing all available profiles for an 8320 switch:

```
switch# show profiles available

Available profiles
------------------
L3-agg   98304 L2 entries 120000 Host entries 16384  Route entries

L3-core  32768 L2 entries 14000  Host entries 131064 Route entries (Default)

Leaf     98304 L2 entries 120000 Host entries 16384  Route entries

Spine    32768 L2 entries 14000 Host entries 131064 Route entries
```

Showing all available profiles for an 8325 switch:

```
switch# show profiles available

Available profiles
```

```
-------------------
L3-agg   98304 L2 entries, 120000 Host entries (8190 unique overlay
          neighbors, 48638 unique underlay neighbors), 29696 Route entries

L3-core  32768 L2 entries, 28000 Host entries (16382 unique overlay
          neighbors, 32766 unique underlay neighbors), 163796 Route entries

Leaf     98304 L2 entries, 120000 Host entries (32766 unique overlay
          neighbors, 12286 unique underlay neighbors), 29696 Route entries
          (Default)

Spine    32768 L2 entries, 28000 Host entries (16382 unique overlay
          neighbors, 32766 unique underlay neighbors), 163796 Route entries
```

Showing all available profiles for a 9300 switch:

```
switch# show profiles available

Available Profiles
-------------------
 DC-Optimized-Leaf   MAC Addresses 81920, Unicast Routes(IPv4: 65536, IPv6:
32768), Host-Routes/Hosts(IPv4: 163840, IPv6: 81920), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765)
(Default)

 DC-Optimized-Spine  MAC Addresses 32768, Unicast Routes(IPv4: 1269760, IPv6:
624640), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742)

 Leaf                MAC Addresses 81920, Unicast Routes(IPv4: 65536, IPv6:
32768), Host-Routes/Hosts(IPv4: 163840, IPv6: 81920), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765), Legacy Profile

 Spine               MAC Addresses 32768, Unicast Routes(IPv4: 1269760, IPv6:
624640), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742), Legacy Profile
```

Showing all available profiles for a 9300S switch:

```
switch# show profiles available

Available Profiles
-------------------
 DC-Optimized-Leaf    MAC Addresses 49152, Unicast Routes(IPv4: 32269, IPv6:
16885), Host-Routes/Hosts(IPv4: 98304, IPv6: 49152), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765)(Default)

 DC-Optimized-Spine   MAC Addresses 32768, Unicast Routes(IPv4: 720527, IPv6:
368404), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742)

 Leaf                 MAC Addresses 49152, Unicast Routes(IPv4: 32269, IPv6:
16885), Host-Routes/Hosts(IPv4: 98304, IPv6: 49152), ARP Entries(Tunnel: 32765,
Non-Tunnel: 32765), Legacy Profile

 Spine                MAC Addresses 32768, Unicast Routes(IPv4: 720527, IPv6:
368404), Host-Routes/Hosts(IPv4: 32768, IPv6: 16384), ARP Entries(Non-Tunnel:
31742), Legacy Profile
```

Starting with AOS-CX 10.16.1005, DC-Optimized-Leaf is the default profile for the 9300 and 9300S Switch Series. DC-Optimized-Leaf and DC-Optimized-Spine profiles do not support IP tunnels, including 6in4 tunnels, 6in6 tunnels, and GRE tunnels.

Showing all available profiles for an 8360 switch:

```
switch# show profiles available

Available profiles
------------------
Aggregation-Leaf   114688 L2 entries, 163840 Host entries, 65536 Route entries

Core-Spine         32768 L2 entries, 65536 Host entries, 630784 Route entries

Leaf-Extended      212992 L2 entries, 16384 Host entries, 65536 Route entries
```

Showing all available profiles for a 10000 switch:

```
switch# show profiles available

Available profiles
------------------
L3-agg   98304 L2 entries, 120000 Host entries (8190 unique overlay
          neighbors, 48638 unique underlay neighbors), 29696 Route entries

L3-core  32768 L2 entries, 28000 Host entries (16382 unique overlay
          neighbors, 32764 unique underlay neighbors), 163796 Route entries

Leaf     98304 L2 entries, 120000 Host entries (32766 unique overlay
          neighbors, 12284 unique underlay neighbors), 29696 Route entries
          (Default)

Spine    32768 L2 entries, 28000 Host entries (16382 unique overlay
          neighbors, 32764 unique underlay neighbors), 163796 Route entries
```

Command History

Release	Modification
10.16.1005	DC-Optimized-Leaf and DC-Optimized-Leaf profiles introduced on 9300 and 9300S Switch series.
10.09	Command Introduced on the 10000.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8320 8325 8325H 8325P	Manager (#)	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8360 9300 9300S 10000		

show profile current

```
show profile current
```

Description

Shows the current system profile.

Examples

Showing the current profile on the 9300 and 9300S:

```
switch# show profile current
Current profile
-------------------
DC-Optimized-Leaf
```

Showing the current profile on the 8320, 8325, or 10000:

```
switch# show profile current

Current profile
-------------------
L3-core
```

Showing the current profile on the 8360:

```
switch# show profile current

Current profile
-------------------
Core-Spine
```

Command History

Release	Modification
10.09	Command Introduced on the 10000.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8320 8325	Manager (#)	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8325H 8325P 8360 9300 9300S 10000		

Restoring the switch to factory default settings

Prerequisites

You are connected to the switch through its Console port.

This procedure erases all user information and configuration settings Consider backing up your running configuration first.

1. Optionally, back up the running configuration with either **copy running-config <*REMOTE-URL*>** or **copy running-config <STORAGE-URL>**. The **json** storage format is required for later configuration restoration.
2. Switch to the configuration context with the command **config**.
3. Erase all user information and configuration, restoring the switch to its factory default state with the command **erase all zeroize**. Enter **Y** when prompted to continue. The switch automatically restarts.
4. Optionally restore your saved configuration (it must be in **json** format) with either **copy <*REMOTE-URL*> running-config** or **copy <STORAGE-URL> running-config** followed by **copy running-config startup-config**.

Example

Backing up the running configuration to a file on a remote server (using TFTP), resetting the switch to its factory default state, and then restoring the saved configuration.

```
switch# copy running-config tftp://192.168.1.10/backup_cfg json vrf mgmt

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10340    0     0  100 10340      0  1329k --:--:-- --:--:-- --:--:-- 1329k
100 10340    0     0  100 10340      0  1313k --:--:-- --:--:-- --:--:-- 1313k
switch#
switch#
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.
[  OK  ] Stopped PSPO Module Daemon.
[  OK  ] Stopped AOS-CX Switch Daemon for BCM.
...
[  OK  ] Stopped Remount Root and Kernel File Systems.
[  OK  ] Reached target Shutdown.
```

```
reboot: Restarting system
Press Esc for boot options
ServiceOS Information:
    Version:          GT.01.03.0006
    Build Date:       2018-10-30 14:20:44 PDT
    Build ID:         ServiceOS:GT.01.03.0006:8ee0faaa52da:201810301420
    SHA:              xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
...

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

Boot Profiles:

0. Service OS Console
1. Primary Software Image [XL.10.02.0010]
2. Secondary Software Image [XL.10.02.0010]

Select profile(primary):

Booting primary software image...
Verifying Image...

Image Info:
        Name: AOS-CX
     Version: XL.10.02.0010
    Build Id: AOS-CX:XL.10.02.0010:feaf5b9b7f09:201901292014
  Build Date: 2019-01-29 12:43:50 PST

Extracting Image...
Loading Image...
Done.
kexec_core: Starting new kernel
System is initializing
fips_post_check[5473]: FIPS_POST: Cryptographic selftest started...SUCCESS
[  OK  ] Started Login banner readiness check.
...
8400X login: admin
Password:

switch#
switch#
switch# copy tftp://192.168.1.10/backup_cfg running-config json vrf mgmt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10340  100 10340    0     0  2858k      0 --:--:-- --:--:-- --:--:-- 2858k
100 10340  100 10340    0     0  2804k      0 --:--:-- --:--:-- --:--:-- 2804k
Large configuration changes will take time to process, please be patient.
switch#
switch#
switch# copy running-config startup-config
Large configuration changes will take time to process, please be patient.
switch#
```

Limitations and considerations

Profile switching between VSX and VSF

- VSF and VSX are mutually exclusive features. Before switching between profiles, ensure the device is in standalone mode.
- Configuration data is not compatible between VSF and VSX profiles. Back up your configurations before changing profiles (switching will erase startup configurations and reboot the device).
- Never apply the VSX profile on an active VSF setup. Applying VSX profile on an active VSF commander may cause undesired behavior and potentially require a factory reset.
- Checkpoints created in one profile mode should not be applied to a switch in a different profile mode. For example, do not apply VSX checkpoints on a switch configured for VSF profile, or vice versa.
- Configuration downloads should match the current profile of the switch. Do not download VSX configurations to a switch in VSF profile mode, or vice versa.

Software downgrade considerations

- When performing a software downgrade on a device configured with either VSX or VSF profiles, ensure that the startup configuration is erased prior to the downgrade process. This prevents configuration incompatibilities that could arise between different software versions.
- Failure to erase the startup configuration before downgrade may result in unexpected behavior, including potential boot failures or feature inconsistencies when the device initializes with the older software version which does not support VSX.

REST API profile switching procedure

Complete the following steps when changing profiles via REST API:

1. Ensure the device is in standalone mode.
2. Execute **erase startup-config**.
3. Set the **configured_profile** in System table to the desired profile (VSX or Basic).
4. Save the configuration.
5. Reboot the switch to activate the desired profile.

It is best practice to always save the running configuration after changing profiles and before rebooting. If the running configuration is not saved after a profile change, a subsequent reboot may return the device to the Basic (default) profile.

Management interface commands

default-gateway

```
default-gateway <IP-ADDR>
no default-gateway <IP-ADDR>
```

Description

Assigns an IPv4 or IPv6 default gateway to the management interface. An IPv4 default gateway can only be configured if a static IPv4 address was assigned to the management interface. An IPv6 default

gateway can only be configured if a static IPv6 address was assigned to the management interface. The default gateway should be on the same network segment.

The **no** form of this command removes the default gateway from the management interface.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255, or IPv6 format (**xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**), where **x** is a hexadecimal number from 0 to F.

Examples

Setting a default gateway with the IPv4 address of **198.168.5.1**:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# default-gateway 198.168.5.1
```

Setting an IPv6 address of **2001:DB8::1**:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# default-gateway 2001:DB8::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config-if-mgmt	Administrators or local user group members with execution rights for this command.

ip static

```
ip static <IP-ADDR>/<MASK>
no ip static <IP-ADDR>/<MASK>
```

Description

Assigns an IPv4 or IPv6 address to the management interface.

The **no** form of this command removes the IP address from the management interface and sets the interface to operate as a DHCP client.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255, or IPv6 format (**xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**), where **x** is a hexadecimal number from 0 to F.
<MASK>	Specifies the number of bits in an IPv4 or IPv6 address mask in CIDR format (**x**), where **x** is a decimal number from 0 to 32 for IPv4, and 0 to 128 for IPv6.

Examples

Setting an IPv4 address of **198.51.100.1** with a mask of **24** bits:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip static 198.51.100.1/24
```

Setting an IPv6 address of **2001:DB8::1** with a mask of **32** bits:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# ip static 2001:DB8::1/32
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config-if-mgmt	Administrators or local user group members with execution rights for this command.

nameserver

```
nameserver <PRIMARY-IP-ADDR> [ <SECONDARY-IP-ADDR> ]
no nameserver <PRIMARY-IP-ADDR> [ <SECONDARY-IP-ADDR> ]
```

Description

Assigns a primary or secondary IPv4 or IPv6 DNS server to the management interface. IPv4 DNS servers can only be configured if a static IPv4 address was assigned to the management interface. IPv6 DNS servers can only be configured if a static IPv6 address was assigned to the management interface. The default gateway should be on the same network segment.

The **no** form of this command removes the DNS servers from the management interface.

Parameter	Description
<PRIMARY-IP-ADDR>	Specifies the IP address of the primary DNS server. Specify the address in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255, or IPv6 format (**xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**), where **x** is a hexadecimal number from 0 to F.
<SECONDARY-IP-ADDR>	Specifies the IP address of the secondary DNS server. Specify the address in IPv4 format (**x.x.x.x**), where **x** is a decimal number from 0 to 255, or IPv6 format (**xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**), where **x** is a hexadecimal number from 0 to F.

Examples

Setting primary and secondary DNS servers with the IPv4 addresses of **198.168.5.1** and **198.168.5.2** :

```
switch(config)# interface mgmt
switch(config-if-mgmt)# nameserver 198.168.5.1 198.168.5.2
```

Setting primary and secondary DNS servers with the IPv6 addresses of **2001:DB8::1** and **2001:DB8::2**:

```
switch(config)# interface mgmt
switch(config-if-mgmt)# nameserver 2001:DB8::1 2001:DB8::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config-if-mgmt	Administrators or local user group members with execution rights for this command.

psm

```
psm  {host <psm-ip-addr-1> <psm-ip-addr-2> <psm-ip-addr-3> [vrf default|mgmt]}| list | no
```

Description

The Pensando Policy and Services Manager (PSM) is a programmable, secure, highly available, centralized system for managing infrastructure policy, with capabilities for:

- Deploying and controlling distributed firewall security
- Telemetry and analytics
- Troubleshooting
- Operations and maintenance: events, alerts, technical support
- Authentication, authorization, and accounting (AAA)

The PSM is designed to establish and manage consistent policies for each 10000 Switch Series Distributed Services Switch (DSS).

Parameter	Description
`host <psm-ip-addr-1> <psm-ip-addr-2> <psm-ip-addr-3>`	Provide the IP addresses for the cluster nodes of the PSM to which the DSS will associate. The maximum number of hosts is three, and best practices is to specify all three.
`vrf default|mgmt`	Define the PSM connectivity type . ■ **default** VRF connectivity is in-band to the PSM ■ **mgmt** VRF connectivity is out-of-band via management VRF to the PSM
`list`	Print a command list
`no`	Negate a command or set its defaults.

Usage

Before associating a DSS with a PSM:

1. Ensure that there will be Layer 3 connectivity between the DSS and the PSM through the management or in-band interface.
2. Make sure that the DSS is not currently associated with another PSM.
3. Verify that the time is set correctly on the switch.

For complete information on the Pensando Policy and Services Manager, refer to the *Pensando Policy and Services Manager for Distributed Services Switches: User Guide*.

The following caveats and limitations apply to a stateful L4 firewall:

- Stateful services for VRFs, where route leaking is enabled, are not supported.
- Port-access (802.1x, MAC authentication, Device Profile), Port-security, DHCP v4/v6 snooping, Dynamic ARP Inspection and/or IPv4/v6 Source Lockdown configurations are mutually exclusive with PSM Stateful firewall policies.
- For locally-switched and routed flows on the switch, the traffic from the host is subject to policy processing only once and only egress policy is enforced on the traffic egressing the workload and entering the switch.

Examples

Configuring a DSS to associate with a PSM with three nodes with the IP addresses 192.168.68.49, 192.168.68.50, and 192.168.68.51

```
switch(config)# psm
switch(config-psm)# host 192.168.68.49 192.168.68.50 192.168.68.51 vrf default
```

Command History

Release	Modification
10.09.100	Command introduced

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show interface mgmt

```
show interface mgmt [vsx-peer]
```

Description

Shows status and configuration information for the management interface.

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

Example

```
switch# show interface mgmt

  Address Mode                  : static
  Admin State                   : up
  Mac Address                   : 02:42:ac:11:00:02
  IPv4 address/subnet-mask      : 192.168.1.10/16
  Default gateway IPv4          : 192.168.1.1
  IPv6 address/prefix           : 2001:db8:0:1::129/64
  IPv6 link local address/prefix: fe80::7272:cfff:fefd:e485/64
  Default gateway IPv6          : 2001:db8:0:1::1
  Primary Nameserver            : 2001::1
  Secondary Nameserver          : 2001::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show psm

```
show psm
```

Description

Show configuring settings that associate a Pensando Policy and Services Manager (PSM) with a 10000 Switch series Distributed Services Switch (DSS).

Examples

The following example shows the PSM configuration on a DSS, where the DSS is associated with a PSM with three nodes with the IP addresses 192.168.68.49, 192.168.68.50, and 192.168.68.51

```
switch(config)#  show psm

Policy and Services Manager Information

Operational Status  : admitted
Host Addresses      : 192.168.68.49, 192.168.68.50, 192.168.68.51
VRF                 : default
Source IP           : 18.127.1.1
```

Command History

Release	Modification
10.09.100	Command introduced

Command Information

Platforms	Command context	Authority
10000	config	Administrators or local user group members with execution rights for this command.

NTP commands

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
```

Command History

Release	Modification
10.07 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.

WARNING: Using "#" in the NTP password will prevent the NTP to syncronize when authentication is enabled

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 F8245a0b 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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp conductor

```
ntp conductor vrf <VRF-NAME> {stratum <NUMBER>]
no ntp conductor vrf <VRF-NAME> {stratum <NUMBER>]
```

Description

Sets the switch as the conductor time source for NTP clients on the specified VRF. By default, the switch operates at stratum level 8. The switch cannot function as both NTP conductor and client on the same VRF.

The **no** form of this command stops the switch from operating as the conductor time source on the specified VRF.

Parameter	Description
`vrf <VRF-NAME>`	Specifies the VRF on which to act as conductor time source.
`stratum <NUMBER>`	Specifies the stratum level at which the switch operates. Range: 1 - 15. Default: 8.

Examples

Setting the switch to act as conductor time source on VRF **primary-vrf** with a stratum level of **9**.

```
switch(config)# ntp conductor vrf primary-vry statum 9
```

Stops the switch from acting as conductor time source on VRF **primary-vrf**.

```
switch(config)# no ntp conductor vrf primary-vry
```

Command History

Release	Modification
10.08	Inclusive language.

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 9300 9300S 10000	`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

Parameter	Description
	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.

When configuring a time backward more than five minutes on the HPE Aruba Networking 8320, 8325, or 9300 Switch Series, a reboot is recommended to avoid unusual switch behavior.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as a radio or atomic clock or a GPS time source).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 time server.

When using multiple servers with same stratum setting, the best practice to configure a preferred server, so NTP will attempt to use the preferred server as the primary NTP connection. If a preferred server is not manually set when NTP is enabled, the configured server with the lowest stratum will automatically be set as the preferred server. If there are servers with the same stratum, this auto prefer status will prevent AOS-CX from toggling between different servers as the primary server. Auto prefer selection of servers with same stratum (if not manually selected) may change after reconfiguring the switch, or after executing the **reboot** command.

Examples

Defining the ntp server pool.ntp.org, using iburst, and NTP version 4.

```
switch(config)# ntp server pool.ntp.org iburst version 4
```

Removing the ntp server pool.ntp.org.

```
switch(config)# no ntp server pool.ntp.org
```

Defining the ntp server my-ntp.mydomain.com and makes it the preferred server.

```
switch(config)# ntp server my-ntp.mydomain.com prefer
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp vrf

```
ntp vrf <VRF-NAME>
no ntp vrf <VRF-NAME>
```

Description

Specifies the VRF on which the NTP client communicates with an NTP server. The switch cannot function as both NTP conductor and client on the same VRF.
The **no** form of the command returns to default VRF.

Parameter	Description
<VRF-NAME>	Specifies the name of a VRF.

Example

Setting the switch to use the default VRF for NTP client traffic.

```
switch(config)# ntp vrf default
```

Setting the switch to use the default management VRF for NTP client traffic.

```
switch(config)# ntp vrf mgmt
```

Returning the switch to use the default VRF for NTP client traffic.

```
switch(config)# no ntp vrf
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp associations

```
show ntp associations [vsx-peer]
```

Description

Shows the status of the connection to each NTP server. The following information is displayed for each server:

- Tally code : The first character is the Tally code:
  - (blank): No state information available (e.g. non-responding server)
  - x : Out of tolerance (discarded by intersection algorithm)
  - . : Discarded by table overflow (not used)
  - - : Out of tolerance (discarded by the cluster algorithm)
  - + : Good and a preferred remote peer or server (included by the combine algorithm)
  - # : Good remote peer or server, but not utilized (ready as a backup source)
  - * : Remote peer or server presently used as a primary reference
  - o : PPS peer (when the prefer peer is valid)
- ID: Server number.
- NAME: NTP server FQDN/IP address (Only the first 24 characters of the name are displayed).
- REMOTE: Remote server IP address.
- REF_ID: Reference ID for the remote server (Can be an IP address).
- ST: (Stratum) Number of hops between the NTP client and the reference clock.
- LAST: Time since the last packet was received in seconds unless another unit is indicated.
- POLL: Interval (in seconds) between NTP poll packets. Maximum (1024) reached as server and client sync.
- REACH: 8-bit octal number that displays status of the last eight NTP messages (377 = all messages received).

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

Example

```
switch# show 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
-------------------------------------------------------------------------
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp authentication-keys

```
show ntp authentication-keys [vsx-peer]
```

Description

Shows the currently defined authentication keys.

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

Examples

```
switch# show ntp authentication-keys
--------------------------------
Auth key  Trusted   MD5 password
--------------------------------
 10          No     **********
 20         Yes     **********
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp servers

```
show ntp servers[vsx-peer]
```

Description

Shows all configured NTP servers, including any DHCP servers, default pool servers or any server with the status **auto prefer**.

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

Example

```
switch# show 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
-----------------------------------------------
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp statistics

`show ntp statistics [vsx-peer]`

Description

Shows global NTP statistics. The following information is displayed:

- Rx-pkts: Total NTP packets received.
- Current Version Rx-pkts: Number of NTP packets that match the current NTP version.
- Old Version Rx-pkts: Number of NTP packets that match the previous NTP version.
- Error pkts: Packets dropped due to all other error reasons.
- Auth-failed pkts: Packets dropped due to authentication failure.
- Declined pkts: Packets denied access for any reason.
- Restricted pkts: Packets dropped due to NTP access control.
- Rate-limited pkts: Number of packets discarded due to rate limitation.
- KOD pkts: Number of Kiss of Death packets sent.

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

Examples

```
switch(config)# show ntp statistics
                Rx-pkts 100
Current Version Rx-pkts 80
    Old Version Rx-pkts 20
             Err-pkts 2
       Auth-failed-pkts 1
          Declined-pkts 0
        Restricted-pkts 0
      Rate-limited-pkts 0
             KoD-pkts 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp status

```
show ntp status [vsx-peer]
```

Description

Shows the status of NTP on the switch.

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

Examples

Displaying the status information when the switch is not synced to an NTP server:

```
switch# show ntp status
NTP is enabled.
NTP authentication is enabled.
NTP is using the default VRF for NTP server connections.

Wed Nov 23 23:29:10 PDT 2016
NTP uptime: 187 days, 1 hours, 37 minutes, 48 seconds

Not synchronized with an NTP server.
```

Displaying the status information when the switch is synced to an NTP server:

```
switch# show ntp status
NTP is enabled.
NTP authentication is enabled.
NTP is using the default VRF for NTP server connections.

Wed Nov 23 23:29:10 PDT 2016
NTP uptime: 187 days, 1 hours, 37 minutes, 48 seconds

Synchronized to NTP Server 17.253.2.253 at stratum 2.
Poll interval = 1024 seconds.
Time accuracy is within 0.994 seconds
Reference time: Thu Jan 28 2016 0:57:06.647 (UTC)
```

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.

Hibernation

Hibernation is a low power state where the switch is not functional. This state is very similar to a power off state, but includes the ability to power on automatically when the pre-configured hibernation period expires, or when the mode button is pressed. When the hibernation period expires, the switch is powered up and booted using the normal boot process.

Hibernation commands

hibernate now

`hibernate now <END-TIME>`

Description

Activates the switch hibernation immediately. There is no network traffic or activity check on the switch. This command is only available on the VSF conductor and the command execution on the VSF conductor dictates the immediate hibernation of the entire stack.

Profile names	Description
<END_TIME>	Specifies the hibernation end-time in MM:DD:hh:mm format.

Usage

If the same switch configurations are expected to be persistent after the wake-up from hibernation, manually save the current running configurations to the start-up configurations before entering the **hibernation now** command.

Hibernation end-time is a required prerequisite to configure immediate hibernation. The switch cannot enter hibernation if an end-time has not been configured. The end-time must be at least five minutes after the current system time to allow for the system to shutdown safely. It is recommended that the end-time is always greater than the total time taken for the system shutdown.

If the system end-time does not exist or is an incomplete format, an error message is displayed on the console and hibernation does not take place.

Examples

Enter immediate hibernation and wake up on 10th September at 8:30 PM.

```
switch(config)# hibernate now 09:10:20:30
Checking if the configuration needs to be saved...

Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.
This command will hibernate the system now and wake up at 2025-09-10 20:30.
During that time, the system will not respond to any network traffic and the
console will be inaccessible. The only way to wake up the switch before the
hibernation period expires will be to press the mode button on the front panel or
to power cycle the switch.
```

Hibernation fails due to syntax error.

```
switch(config)# hibernate now 09:10:20
The specified hibernation end-time is invalid. This command requires the
hibernation end-time in MM:DD:hh:mm format.
```

Hibernation fails because the end-time is less than five minutes from the current system time.

```
switch(config)# show clock
Tue Feb 28 11:59:00 UTC 2025
System is configured for timezone : UTC
switch(config)# hibernate now 02:28:00:00
The specified hibernation end-time needs to be more than 5 minutes from the
current time.
```

Hibernation fails because the end-time is more than 365 days from the current system time.

```
switch(config)# show clock
Tue Mar 1 00:00:00 UTC 2025
System is configured for timezone : UTC
switch(config)# hibernate now 03:01:00:00
The specified hibernation end-time needs to be at most 365 days from the current
time.
```

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
8325H 9300S	config	Administrators or local user group members with execution rights for this command.

hibernate periodic

```
hibernate periodic <RECURRING-DAYS> <START_TIME-END_TIME>
no hibernate periodic <RECURRING-DAYS> <START_TIME-END_TIME>
```

Description

Enables recurring hibernation mode and configures recurring hibernation options, but it does not hibernate the switch immediately. The configurations are saved as part of the running configuration. To enable recurring hibernation on every hibernation cycle, manually save the configurations. This command is only available on the VSF conductor and the configurations on VSF conductor are retrieved by the entire stack when hibernation mode is triggered.

The **no** form of this command disables recurring hibernation.

Profile names	Description
<RECURRING_DAYS>	Specify the recurrence of hibernation. The options are daily, sunday, monday, tuesday, wednesday, thursday, friday, saturday, weekdays, and weekend.
<START_TIME-END_TIME>	Specify the hibernation start-time and end-time in "HH:MM-HH:MM format, up to 10 entries.

Usage

This command allows recurring days to be set as daily, weekdays only, weekend only, or each individual day of the week. It is possible to have seven different profiles catered for each individual day of the week or different profiles for weekdays versus weekend according to business requirements. Each individual day of the week may have up to 10 sets of hibernation configuration timings.

This command enforces the following rules for input parameters:

The end time must always be at least 5 minutes from the start time.

Overlapping time periods are allowed.

To configure for continuous days of hibernation, the user must always ensure that the end time of the last hibernation configuration of a previous day is less than 5 minutes from the start time of the first hibernation configuration of a following day.

If one or more the specified parameters is invalid, an error message is displayed on the console and recurring hibernation configurations is not saved.

The **no** form of this command without the extra parameter disables recurring hibernation. The extra parameter allows the user to disable recurring hibernation and clear configs on a specific day of the week or weekdays or weekend only. There is no need for a reboot for the recurring hibernation disablement to take effect. Manually save the current running configurations to the start-up configurations for them to take affect on the next reboot.

Examples

Enable recurring hibernation mode.

```
switch(config)# hibernate periodic
This command will enable recurring hibernation mode and hibernate the system
according to the configured recurring hibernation start-time and end-time. During
that time, the system will not respond to any network traffic and the console will
be inaccessible. The only way to wake up the switch before the hibernation period
expires will be to press the mode button on the front panel or to power cycle the
switch.

Continue (y/n)?
```

Hibernate every Monday from 12AM to 9PM.

```
switch(config)# hibernate periodic monday
switch(config-hibernate-mon)# time-period 00:00-09:00
```

Hibernate every Monday from 12AM to 9AM, 12PM to 3 PM, and 7PM to 11:59PM.

```
switch(config)# hibernate periodic monday
switch(config-hibernate-mon)# time-period 00:00-09:00
switch(config-hibernate-mon)# time-period 12:00-15:00
switch(config-hibernate-mon)# time-period 19:00-23:59
```

Hibernate the whole weekend and wake up on Monday 9:00 AM.

```
switch(config)# hibernate periodic weekend
switch(config-hibernate-weekend)# time-period 00:00-23:59
switch(config-hibernate-weekend)# no hibernate periodic monday
This command will clear hibernation configurations for monday only.
Continue (y/n)? y
```

Clear all recurring hibernation configurations.

```
switch(config)# no hibernate periodic daily
This command will clear all hibernation configurations.
Continue (y/n)? y
```

Clear hibernation configurations for weekends.

```
switch(config)# no hibernate periodic weekend
This command will clear all hibernation configurations for weekend only.
Continue (y/n)? y
```

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
8325H 9300S	config	Administrators or local user group members with execution rights for this command.

show hibernation

```
show hibernation
```

Description

Displays the current hibernation configuration and the upcoming hibernation schedule on the switch

Examples

Display the current hibernation configuration. Enter immediate hibernation and wake up on 10th September at 8:30 PM.

```
switch# show hibernation
Recurring hibernation: Disabled
Recurring configurations:
        Monday:
                00:00 to 08:00
        Saturday:
                00:00 to 09:00
                12:00 to 14:00
                18:00 to 23:59
        Sunday:
                00:00 to 09:00
                12:00 to 23:59
Upcoming hibernation time : NONE
Upcoming wake-up time     : NONE
```

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
8325H 9300S	config	Administrators or local user group members with execution rights for this command.

show running-config (hibernation)

```
show running-config (hibernation)
```

Description

Displays the current non-default configuration on the switch. Default hibernation configurations are not displayed in the running-config context.

Examples

Display the current non-default hibernation configurations on the switch.

```
switch# show running-config
Current configuration:
!
!Version AOS-CX FL.10.16.0000
!export-password: default
hostname switch
hibernate periodic
hibernate periodic monday
        time-period 00:00-08:00
hibernate periodic saturday
        time-period 00:00-09:00
        time-period 12:00-14:00
        time-period 18:00-23:59
hibernate periodic sunday
        time-period 00:00-09:00
        time-period 12:00-23:59
interface 1/1/1
        no shutdown
        no routing
        vlan access 1
interface 1/1/2
        no shutdown
        no routing
        vlan access 1
```

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
8325H 9300S	config	Administrators or local user group members with execution rights for this command.

Client probe and configuration

Client probing allows the switch to wake up silent clients it is connected to. A silent client is one that doesn't send any packet to allow a switch to authenticate the client until probed. These clients may send packets on a link up but will stop sending packets once they enter power saving mode (i.e., sleep mode).

Client probing provides the following benefits:

- The switch port can be the source of the probe packets that can wake up silent clients. This eliminates the need for dedicated device in the network to generate the probe packets. It also reduces the amount of BUM traffic in the network otherwise used to wake up silent clients.
- Control the type of probe packets to be sent, how often to send them and when to stop.
- The data to be used in the probe packets. Some of the clients such as industrial weighing scales do not respond to any random probe packet. They must be probed with the broadcast IP address of the subnet associated with the IP assigned to them.

Client probing commands

(remote) associate profile

```
associate profile {sftp user <username> password [ciphertext <CIPHERTEXT-PASSWORD>
plaintext <PLAINTEXT PASSWORD> | tftp]} {host <IP-ADDR | FQDN>} [port <PORT>] {file
<FILE-PATH> [vrf<VRF-NAME>]
no associate profile {sftp user <username> password [ciphertext <CIPHERTEXT-PASSWORD>
plaintext <PLAINTEXT PASSWORD> | tftp]} {host <IP-ADDR | FQDN>} [port <PORT>] {file
<FILE-PATH> [vrf<VRF-NAME>]
```

Description

Configures how profile information used in probe packets is obtained. The default setting obtains information from a remote file via tftp or sftp.

The **no** form sets to default configuration.

Usage

The switch uses the name of the remote file to create a profile. Make sure the remote file follows proper naming requirements.

Parameter	Description
USERNAME	Specifies the username, which must be between 2 and 64 characters in length.
CIPHERTEXT-PASSWORD	Specifies the password. Maximum of 64 characters.
PLAINTEXT-PASSWORD	Specifies the password. Maximum of 64 characters.
IP-ADDR|FQDN	Specifies the remote server IP address or hostname.
PORT	Sets the sftp or tftp port number. sftp default: 22 tftp default: 69
FILE-PATH	Specifies the file name to be copied.

Parameter	Description
VRF-NAME	(Default) Specifies the VRF to be used for reaching the remote server.

Examples

Configuring the client-probe profile to an SFTP location with standard SFTP port 22:

```
switch(config)# client probe
switch(config-cp)# associate profile sftp user johndoe password plaintext hello
host 20.20.20.1 file client-info.json
```

Configuring the client-probe profile to an SFTP location hosted on custom SFTP port 3333:

```
switch(config)# client probe
switch(config-cp)# associate profile sftp user johndoe password plaintext hello
host 20.20.20.1 port 3333 file client-info.json
```

To configure a remote profile, provide a JSON profile to a **remote_server**, using the following format:

```
[
{
       "vlan": "<VLAN-ID>",
       "enable": true|false,
       "source_mac": "<MAC-ADDR>",
       "source_ip": "<IP-ADDR>",
       "broadcast_ip": "<IP-ADDR>",
       "directed_ip_range": {
       "start_ip": "<IP-ADDR>",
       "end_ip": "<IP-ADDR>"
       },
       "directed_ip_list": [
        "<IP-ADDR>",
       ...
       ...
       "<IP-ADDR>"
       ]
 },
 ...
 ...
]
```

Configuring a remote profile:

```
[
 {
       "enable": true,
       "vlan": "10",
       "source_mac": "aa:bb:cc:dd:ee:10",
       "source_ip": "10.0.10.1",
       "broadcast_ip": "10.0.10.255"
 },
 {
       "enable": true,
```

```
        "vlan": "30",
        "source_mac": "aa:bb:cc:dd:ee:30",
        "source_ip": "10.0.30.1",
        "directed_ip_range": {
        "start_ip": "10.0.30.2",
        "end_ip": "10.0.30.30"
 }
},
{
        "enable": true,
        "vlan": "50",
        "source_mac": "aa:bb:cc:dd:ee:50",
        "source_ip": "10.0.50.1",
        "broadcast_ip": "10.0.50.255",
        "directed_ip_list": [
        "10.0.50.2",
        "10.0.50.7"
],
        "directed_ip_range": {
         "start_ip": "10.0.50.11",
         "end_ip": "10.0.50.30"
}
}
]
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	`config-cp`	Administrators or local user group members with execution rights for this command.

client-probe profile force-download

`client-probe profile force-download`

Description

Enables a user to immediately force download a remote profile rather than waiting until the next cycle of **remote-server refresh-interval** timer.

Example

Force-downloading a remote profile:

```
switch# client probe profile force-download
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

remote-server refresh interval

```
remote-server refresh interval <ID>
no remote-server refresh interval <ID>
```

Description

Configures the time period, in seconds, when the switch will periodically obtain the latest version of the probe profile file from the remote location.

Parameter	Description
<ID>	Time interval, in seconds, to wait before refreshing the client probing data from the source. Default: 3600 seconds

Example

Configuring the switch to refresh the probe data from the remote location every 3600 seconds:

```
switch(config)# client probe
switch(config-cp)# remote-server refresh-interval 3600
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H	config-cp	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8360 10000		

client-probe autogen-probe-file force-regen

```
client-probe autogen-probe-file force-regen
```

Description

Forces the switch to regenerate the probe file. By default, the probe file is regenerated every 30 seconds when enabled.

Examples

Forcing the switch to regenerate the probe file:

```
switch# client probe autogen-probe-file force-regen
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

autogen-enable

```
autogen-enable
no autogen-enable
```

Description

Enables the auto-generation of the client probe file on the switch.

The **no** form disables the auto-generation of the probe file on the switch.

Examples

Enabling auto-generation of the probe file:

```
switch(config)# client probe
switch(config-cp)# autogen-probe-file
switch(config-cp-autogen)# autogen-enable
```

Disabling auto-generation of the probe of the probe file:

```
switch(config)# client probe
switch(config-cp)# autogen-probe-file
switch(config-cp-autogen)# no autogen-enable
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 8400 10000	config-cp-autogen	Administrators or local user group members with execution rights for this command.

autogen-probe-file

```
autogen-probe-file
no autogen-probe-file
```

Description

Configures the switch to automatically generate and host the probe JSON file using L3 configurations. The **no** form sets to default configuration.

Examples

Configuring the switch to automatically generate the profile file context:

```
switch(config)# client probe
switch(config-cp)# autogen-probe-file
switch(config-cp-autogen)#
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100	config-cp	Administrators or local user group members with execution

Platforms	Command context	Authority
8320 8325 8325H 8360 8400 10000		rights for this command.

show client probe autogen-probe-file

```
show client probe autogen-probe-file [FILENAME]
```

Description

Displays the information associated with the auto-generate probe file.

Parameter	Description
<FILENAME>	Specifies the name of the profile.

Example

Showing command output when the file is successfully auto-generated:

```
switch#  show client probe autogen-probe-file

Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Success
Last Generation Attempt      : Thu Aug 22 08:10:47 UTC 2025
Last Successful Generation   : Thu Aug 22 08:10:47 UTC 2025

Generated Probe File
--------------------

[
   {
      "broadcast_ip": "40.0.0.255",
      "directed_ip_range": {
        "end_ip": "40.0.0.254",
        "start_ip": "40.0.0.1"},
      "enable": true,
      "source_ip": "40.0.0.1",
      "source_mac": "18:7a:3b:1b:08:00",
      "vlan": "10"},
   {
      "broadcast_ip": "20.0.0.255",
      "directed_ip_range": {
        "end_ip": "20.0.0.254",
        "start_ip": "20.0.0.1"},
      "enable": true,
      "source_ip": "20.0.0.1",
      "source_mac": "18:7a:3b:1b:08:00",
      "vlan": "20"}]
```

Showing command output with a specified file name:

```
switch#  show client probe autogen-probe-file probe_data.json

Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Success
Last Generation Attempt      : Thu Aug 22 08:10:47 UTC 2025
Last Successful Generation   : Thu Aug 22 08:10:47 UTC 2025

Generated Probe File

---------------------
[
   {
      "broadcast_ip": "40.0.0.255",
      "directed_ip_range": {
        "end_ip": "40.0.0.254",
        "start_ip": "40.0.0.1"},
      "enable": true,
      "source_ip": "40.0.0.1",
      "source_mac": "18:7a:3b:1b:08:00",
      "vlan": "10"},
   {
      "broadcast_ip": "20.0.0.255",
      "directed_ip_range": {
        "end_ip": "20.0.0.254",
        "start_ip": "20.0.0.1"},
      "enable": true,
      "source_ip": "20.0.0.1",
      "source_mac": "18:7a:3b:1b:08:00",
      "vlan": "20"}]
```

Showing command output when auto file generation fails due to unconfigured VLANs:

```
switch#  show client probe autogen-probe-file
Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Failed, No VLAN configured
Last Generation Attempt      : Fri May 09 16:21:27 UTC 2025
Last Successful Generation   : N/A
```

Show command output when the auto file generation fails due to one or more VLANs missing IP configurations.

```
switch#  show client probe autogen-probe-file
Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Failed, VLAN missing IP configuration (1,3,10-15)
Last Generation Attempt      : Thu Aug 22 08:10:47 UTC 2025
Last Successful Generation   : N/A
```

Showing command output when auto file generation fails due to one or more missing VLANs:

```
switch#  show client probe autogen-probe-file
```

```
Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Failed, VLAN not available (1,3,10-15,18)
Last Generation Attempt      : Thu Aug 22 08:10:47 UTC 2025
Last Successful Generation   : N/A
```
```
switch#  show client probe autogen-probe-file

Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Failed, VLAN not available (1,3,10-15,18)
Last Generation Attempt      : Thu Aug 22 08:10:47 UTC 2025
Last Successful Generation   : Thu Aug 22 08:09:47 UTC 2025
```
```
switch#  show client probe autogen-probe-file

Client-Probe File Information

Name                         : probe_data.json
Auto-Generation Status       : Failed, VLAN not available (11,13,17,19,21,23,...)
Last Generation Attempt      : Wed May 07 05:56:38 UTC 2025
Last Successful Generation   : Wed May 07 05:50:06 UTC 2025
```

Showing command output when auto file generation fails due to storage exhaustion:

```
switch#  show client probe autogen-probe-file
Client-Probe File Information

Name                         : client-probe.json
Auto-Generation Status       : Failed, No space left on device
Last Generation Attempt      : Tue Jul 22 08:16:14 UTC 2025
Last Successful Generation   : N/A
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 8400 10000	`config`	Administrators or local user group members with execution rights for this command.

vlans

`vlans <VLAN-RANGE>`

```
no vlans <VLAN-RANGE>
```

Description

Specifies the list of VLANs to be used when generating the probe data.

The **no** form sets it to the default setting.

Example

Enabling probe data generation on a range of VLANs:

```
switch(config)# client probe
switch(config-cp)# autogen-probe-file
switch(config-cp-autogen)# vlans 1,2,35,10,8
switch(config-cp-autogen)# vlans 50-60,80-90
switch(config-cp-autogen)# vlans 100-120,125,128,130-150,159
```

Only 32 VLANS profiles can be generated.

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 8400 10000	config-cp-autogen	Administrators or local user group members with execution rights for this command.

name

```
name <FILENAME>
no name <FILENAME>
```

Description

Specifies the name to be used for the auto-generated probe file. If the filename is not provided, default filename **client-probe.json** will be used. The filename must follow naming requirements.

The **no** form sets to default configuration.

Usage

Filename requirements:

- must be between 2 and 128 characters
- only alphanumeric characters can be used (e.g. a-z, A-Z, 0-9)

- may use underscores (_)
- may use hyphens (-)
- may have a .json extension

Parameter	Description
FILENAME	Specifies the name of the auto-generated probe file. Minimum characters: 2 Maximum characters: 128 Default: client-probe.json

Example

Specifying the name of the probe file:

```
switch(config)# client probe
switch(config-cp)# autogen-probe-file
switch(config-cp-autogen)# name probe_data.json
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 8400 10000	`config-cp-autogen`	Administrators or local user group members with execution rights for this command.

(local) profile

```
profile <PROFILE-NAME>
no profile <PROFILE-NAME>
```

Description

Creates a local or remote profile and enters the profile context.

Parameter	Description
<PROFILE-NAME>	Specifies the name of the profile.

Example

Configuring a new local profile:

```
switch(config)# client probe
switch(config-cp)# profile WakeUp-Clients
switch(config-cp-profile)#
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	config-cp	Administrators or local user group members with execution rights for this command.

entry

```
entry <ENTRY-ID> {vlan <VLAN-ID> | source-mac <MAC-ADDR> | source-ip <IPV4-ADDR> |
broadcast-ip <IPV4-ADDR> | directed-ip-range <START-IPV4-ADDR> <END-IPV4-ADDR> |
directed-ip-list <IPV4-ADDR>}
no entry <ENTRY-ID> {vlan <VLAN-ID> | source-mac <MAC-ADDR> | source-ip <IPV4-ADDR> |
broadcast-ip <IPV4-ADDR> | directed-ip-range <START-IPV4-ADDR> <END-IPV4-ADDR> |
directed-ip-list <IPV4-ADDR>}
```

Description

Configures entries in the profile.

Parameter	Description
vlan	(Mandatory) Specifies the VLAN ID associated with the entry. By default the switch will send probe packets for all the entries in the JSON. But this can be restricted to only certain VLANs using the **vlan-list** configuration.
source-mac	Specifies the source MAC address to use in the probe packets. If omitted, the system MAC address is used in the probe packets.
source-ip	(Mandatory) Specifies the source IP address to use in the probe packets.
broadcast-ip	Specifies the broadcast IP address to use when ping-broadcast probe is enabled.
directed-ip-range	Specifies the range of destination IP address to use when ping-sweep probe is enabled. Only IPv4 subnets from /8 to /32 are supported.
directed-ip-list	Specifies the list of destination IP addresses to use when the ping-

Parameter	Description
	unicast probe is enabled. A maximum of 255 addresses can be used. Only a single address can be specified at a time and the command must be repeated for every address that must be added to the list. If the limit is exceeded, the switch will discard the profile.
<ENTRY-ID>	Specifies the entry ID.
<VLAN-ID>	Specifies the VLAN ID.
<MAC-ADDR>	Specifies the source MAC address.
<IPV4-ADDR>	Specifies the selected IP address.
<START-IP-ADDR>	First IP address in the range.
<END-IP-ADDR>	Last IP address in the range

For a profile to be deemed valid, it must contain one of the following keys: broadcast-ip, directed-ip-range, or directed-ip-list.

If any of the mandatory attributes are not configured, the entry will be treated as incomplete and the profile will not be used.

Example

Configuring local profile entries:

```
switch(config)# client probe
switch(config-cp)# profile WakeUp-Clients
switch(config-cp-profile)# entry 1
switch(config-cp-profile-entry)# vlan 30
switch(config-cp-profile-entry)# source-mac aa:bb:cc:dd:ee:30
switch(config-cp-profile-entry)# source-ip 10.0.30.1
switch(config-cp-profile-entry)# broadcast-ip 10.0.30.255
switch(config-cp-profile-entry)# directed-ip-range 10.0.30.2 10.0.30.30
switch(config-cp-profile)# entry 2
switch(config-cp-profile-entry)# vlan 50
switch(config-cp-profile-entry)# source-ip 10.0.50.1
switch(config-cp-profile-entry)# directed-ip-list 10.0.50.2
switch(config-cp-profile-entry)# directed-ip-list 10.0.50.7
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	`config-cp-profile-entry`	Administrators or local user group members with execution rights for this command.

probe-duration

```
probe-duration [periodic | client-detection]
no probe duration [periodic | client-detection]
```

Description

Configures how long the switch will probe for clients. The switch stops probing once the client is detected on a port, or continues probing if one or more clients are detected on the port. The timer default is periodic.

Example

Configuring the switch to stop probing once a client is detected on the port:

```
switch(config)# client probe
switch(config-cp)# probe-duration client-detection
```

When probe duration is configured as "client-detection", the probe packets will stop after the first client is detected on the interface. If there are other silent clients on the same interface, they will no longer see any probe packets and may not awoken. It is recommended to use the probe duration as "periodic" if multiple silent clients can be connected on the same interface.

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	`config-cp`	Administrators or local user group members with execution rights for this command.

probe-interval

```
probe-interval <ID>
no probe-interval <ID>
```

Description

Configures the time period, in seconds, for the switch to wait before probing for clients again.

Parameter	Description
`<ID>`	Specifies the interval between consecutive probes, in seconds. Default: 60 seconds.

Example

Configuring the switch to send probe packets every 30 seconds:

```
switch(config)# client probe
switch(config-cp)# probe-interval 30
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	`config-cp`	Administrators or local user group members with execution rights for this command.

probe-type

```
probe-type {ping-broadcast | ping-unicast | ping-sweep | garp}
```

Description

Configures up to multiple packet types to use for probing. The switch sends a packet of each configured type per probe cycle.

Example

Configuring the switch to send probe of all packet types:

```
switch(config)# client probe
switch(config-cp)# probe-type ping-broadcast ping-unicast ping-sweep garp
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	config-cp	Administrators or local user group members with execution rights for this command.

vlan-list

```
vlan-list [unsecure {port|all}] [secure {port|all}]
no vlan-list [unsecure {port|all}] [secure {port|all}]
```

Description

Configures VLANs in the profile to use when probing on the port. The VLANs can be configured for two modes of the port. The first mode, "unsecured" is when the port is not secured by port-access (i.e., no authenticated client on the port). the second mode, "secured" is when the port is secured by port-access (i.e., there is at least one authenticated client on the port). The VLANs can be configured differently for each mode. Use "all" if the switch must send probes for all the VLANs in the profile and "port" when the switch must send probes for only those VLANs of which the port is a member.

The **no** form disables VLANs in the profile to use when probing on the port.

Example

Configuring the switch to use VLANs associated with the port for probing in both secure and unsecure mode:

```
switch(config)# client probe
switch(config-cp)# vlan-list unsecure port secure port
```

Configuring the switch to use all the VLANs associated with the port for probing when not secured, and switch to VLANs associated with the port once secured:

```
switch(config)# client probe
switch(config-cp)# vlan-list unsecure all secure port
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	config-cp	Administrators or local user group members with execution rights for this command.

client probe enable

```
client probe enable
no client probe enable
```

Description

Enables client probing on a port. Client probing must also be enabled globally for it to be operational.

Example

Enabling client probing on the switch:

```
switch(config)# client probe
switch(config-cp)# enable
```

Enabling client probe on a physical interface:

```
switch(config)# interface  1/1/1
switch(config-if)# client probe enable
```

Enabling client probe on a LAG interface:

```
switch(config)# interface lag 1
switch(config-lag-if)# client probe enable
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	config-if	Administrators or local user group members with execution rights for this command.

show client probe profile

```
show client probe profile [PROFILE-NAME]
```

Description

Displays the information associated with the client probe profile.

Parameter	Description
<PROFILE-NAME>	Specifies the name of the profile.

Example

Showing all profiles on the switch:

```
switch# show client probe profile

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                     : probe-info
Type                     : Downloaded
Download Status          : Completed
Last Download Attempt    : Thu Aug 22 09:08:47 UTC 2024
Last Successful Download : Thu Aug 22 09:08:47 UTC 2024
Profile Status           : In Use
Entry ID: 1
------------
VLAN       : 50
Source MAC : aa:bb:cc:dd:ee:50
IPv4
-----
Source IP         : 10.0.50.1
Broadcast IP      : 10.0.50.255
Directed IP List  : -
Directed IP Range : -
Entry ID: 2
------------
VLAN       : 30
Source MAC : aa:bb:cc:dd:ee:50
IPv4
-----
Source IP         : 10.0.50.1
Broadcast IP      : -
Directed IP List  : 10.0.50.2, 10.0.50.7, 10.0.50.8, 10.0.50.7, ...
Directed IP Range : -
Entry ID: 3
------------
VLAN       : 40
Source MAC : aa:bb:cc:dd:ee:50
IPv4
-----
Source IP         : 10.0.40.1
Broadcast IP      : -
Directed IP List  : -
Directed IP Range : 10.0.40.11 - 10.0.40.30
```

Showing a local profile on the switch:

```
switch# show client probe profile

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                       : WakeUp-Clients
Type                       : Local
Download Status            : N/A
Last Download Attempt      : N/A
Last Successful Download   : N/A
Profile Status             : In Use
```

```
Entry ID: 1
------------
VLAN                        : 10
Source MAC                  : aa:bb:cc:dd:ee:10
IPv4
-----
Source IP                   : 10.0.10.1
Broadcast IP                : 10.0.10.255
Directed IP List            : -
Directed IP Range           : -
Entry ID: 2
------------
VLAN                        : 30
Source MAC                  : aa:bb:cc:dd:ee:30
IPv4
-----
Source IP                   : 10.0.30.1
Broadcast IP                : 10.0.30.255
Directed IP List            : -
Directed IP Range           : 10.0.30.2 - 10.0.30.30
Entry ID: 3
------------
VLAN                        : 50
Source MAC                  : aa:bb:cc:dd:ee:50
IPv4
-----
Source IP                   : 10.0.50.1
Broadcast IP                : 10.0.50.255
Directed IP List            : 10.0.50.2, 10.0.50.7
Directed IP Range           : 10.0.50.11 - 10.0.50.30
```

Showing a local profile with invalid entries on the switch:

```
switch# show client probe profile

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                        : WakeUp-Clients
Type                        : Local
Download Status             : N/A
Last Download Attempt       : N/A
Last Successful Download    : N/A
Profile Status              : Error
Entry ID: 1
------------
VLAN                        : 10
Source MAC                  : aa:bb:cc:dd:ee:10
IPv4
-----
Source IP                   : 10.0.10.1
Broadcast IP                : 10.0.10.255
Directed IP List            : -
Directed IP Range           : -
Entry ID: 2*
------------
VLAN                        : 30
Source MAC                  : aa:bb:cc:dd:ee:30
IPv4
```

```
-----
Source IP                    : 10.0.30.1
Broadcast IP                 : -
Directed IP List             : -
Directed IP Range            : -
Entry ID: 3
------------
VLAN                         : 50
Source MAC                   : aa:bb:cc:dd:ee:50
IPv4
-----
Source IP                    : 10.0.50.1
Broadcast IP                 : 10.0.50.255
Directed IP List             : 10.0.50.2, 10.0.50.7
Directed IP Range            : 10.0.50.11 - 10.0.50.30
Entry ID: 4*
------------
VLAN                         : -
Source MAC                   : aa:bb:cc:dd:ee:70
IPv4
-----
Source IP                    : 10.0.70.1
Broadcast IP                 : 10.0.70.255
Directed IP List             : 10.0.70.2, 10.0.70.7
Directed IP Range            : 10.0.70.11 - 10.0.70.30
```

Showing a specific profile on the switch:

```
switch# show client probe profile remote

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                      : remote
Type                      : Downloaded
Download Status           : Failed, VRF not operational
Last Download Attempt     : Thu Aug 22 08:08:47 UTC 2024
Last Successful Download  : N/A
Profile Status            : Pending

switch# show client probe profile remote

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                      : remote
Type                      : Downloaded
Download Status           : Completed
Last Download Attempt     : Thu Aug 22 08:10:47 UTC 2024
Last Successful Download  : Thu Aug 22 08:10:47 UTC 2024
Profile Status            : Error, File parsing failed

switch# show client probe profile remote

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                      : remote
```

```
Type                      : Downloaded
Download Status           : Pending, VRF not available
Last Download Attempt     :
Last Successful Download  :
Profile Status            : Pending

switch# show client probe profile remote

Client-Probe Profile Information

Entries that are not valid are indicated with a '*'.

Name                      : remote
Type                      : Downloaded
Download Status           : Failed, Connection timeout
Last Download Attempt     : Thu Aug 22 09:02:47 UTC 2024
Last Successful Download  : Thu Aug 22 08:35:22 UTC 2024
Profile Status            : In Use
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	`config`	Administrators or local user group members with execution rights for this command.

show client probe statistics

`show client probe statistics [interface <IFRANGE>]`

Description

Displays the statistics associated with client probing.

Parameter	Description
<IFRANGE>	Specifies the interface identifier range.

Example

Showing client probe statistics on all enabled interfaces:

```
switch# show  client  probe statistics

Client-Probe Statistics
```

```
Interface 2/1/10
----------------
Ping Unicast          : 0
Ping Broadcast        : 3441
Ping Sweep            : 225482321
GARP                  : 225502494

Total Probe Cycles    : 107

Interface 2/1/11
----------------
Ping Unicast          : 0
Ping Broadcast        : 3441
Ping Sweep            : 225482321
GARP                  : 225502494

Total Probe Cycles    : 107

Interface 2/1/11
----------------
Ping Unicast          : 0
Ping Broadcast        : 3441
Ping Sweep            : 225482321
GARP                  : 225502494

Total Probe Cycles    : 107
```

Showing client probe statistics on a given interface:

```
switch# show client  probe statistics interface 2/1/10

Client-Probe Statistics

Interface 2/1/10
----------------
Ping Unicast          : 0
Ping Broadcast        : 3442
Ping Sweep            : 225550786
GARP                  : 225568028

Total Probe Cycles    : 107
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H	Manager (#)	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8360 10000		

clear client probe statistics

```
clear client probe statistics [interface [<IFRANGE>]]
```

Description

Clears the statistics associated with client probing.

Parameter	Description
<IFRANGE>	Specifies the interface identifier range.

Example

Clearing client probe statistics on all enabled interfaces:

```
switch# clear client probe statistics
```

Clearing client probe statistics on a given interface:

```
switch# clear client probe statistics interface 1/1/1
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

show running-config

```
show running-config
```

Description

Shows the current running configuration.

Example

Showing the current running configuration for a local profile:

```
switch# show running-config
Current configuration:
!
...
client probe
 probe-type ping-broadcast ping-unicast ping-sweep garp
 probe-interval 50
 probe-duration client-detection
 vlan-list unsecure port secure port
 profile WakeUp-Clients
   entry 1
     vlan 30
     source-mac aa:bb:cc:dd:ee:30
     source-ip 10.0.30.1
     broadcast-ip 10.0.30.255
     directed-ip-range 10.0.30.2 10.0.30.30
   entry 2
     vlan 50
     source-ip 10.0.50.1
     directed-ip-list 10.0.50.2
     directed-ip-list 10.0.50.7
enable
...

interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    client probe enable
...
```

Showing the running configuration for a remote profile:

```
switch# show running-config
Current configuration:
!
...
client probe
  associate profile sftp user admin password plaintext xyz host 20.20.20.1 port
3333 file     client-info.json vrf cp
  remote-server refresh-interval 80
  probe-type ping-broadcast ping-unicast ping-sweep garp
  probe-interval 50
  probe-duration client-detection
  vlan-list unsecure port secure port
  enable
...

interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    client probe enable
```

Showing running configuration for autogen client probe profile:

```
switch# show running-config client-probe
client probe
```

```
   autogen-probe-file
      name 8m-VSF
      vlans 33,3000-3002
      autogen-enable
   enable
```

Showing running configuration for all:

```
switch# show running-config all
Current configuration:
!
...
client probe
 no associate profile
 remote-server refresh-interval 300
 no probe-type
 probe-interval 60
 probe-duration periodic
 no enable
 ...

interface lag 1
 no shutdown
 no routing
 vlan access 1
 ...
 no client probe enable

interface 1/1/1
 no shutdown
 no routing
 vlan access 1
 ...
 no client probe enable
 ...
...
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8360 10000	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

Client-probe limitations

- Only one profile type can be active at a time. Either a local profile or a remote profile must be configured, but not both. If both profiles are configured simultaneously, the profile configured second will be placed in an error state.
- Avoid using the same name for both a local profile and a remote profile. Doing so can cause issues when restoring a configuration checkpoint containing one profile over an existing configuration that contains the other. Since the system identifies profiles solely by name (without considering the type), the local profile may be unintentionally deleted during the restore process.
- When enabling VSX configuration synchronization for Client Probe, ensure that the corresponding ports on the secondary device are configured as Layer 2 (L2). If the interfaces are not set to L2, the Client Probe configuration will be synced but will remain non-operational on the secondary device.
- The remote server refresh interval timer state is not retained across an ISSU. The timer is restarted after the ISSU completes.
- If the profile includes more than 1000 IP addresses, the configured probe interval may not allow a complete probe cycle to finish. Probes are sent in batches of 2 seconds, During each batch, all client probe-enabled ports are probed sequentially in a queue, with each port sending up to 1000 probes over a 2-second duration, with a 2-second pause between batches.
- When setting up a local profile, make sure the client probe feature is disabled before adding or updating entries. If the feature is enabled, any addition or modification will restart probing on all ports where client probe is active.
- The autogeneration of the probe file is supported only on selected switches and does not support unicast probe type or IPv6 addresses.
- The autogeneration of the probe file fails if the device storage usage is more than 90% of total allocation.

The profile name derives from the remote filename, excluding any directory path and stripping the .json extension, if present. For example, if the remote file path is **/work/probing/probe.json**, the selected profile name is **probe**.

Chapter 4
Telnet access

Telnet server enables switches to accept Telnet connections from clients to manage the switch. The user authentication is password based authentication (RADIUS, TACACS+ or locally stored password). The Telnet server can be enabled on a desired VRF using the `telnet server` command. The maximum number of Telnet sessions per VRF is five.

In the default configuration, Telnet access is disabled.

Telnet commands

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
```

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
```

The following example shows the Telnet sessions on all VRFs. If only the **default** VRF is supported by the switch, only the **default** VRF will display in the output of this command.

```
switch(config)# show telnet server sessions all-vrfs
TELNET sessions on VRF mgmt:

    IPv4 TELNET Sessions:
        Server IP        : 10.1.1.1
        Client IP        : 10.1.1.2
        Client Port      : 58835

TELNET sessions on VRF default:

    IPv4 TELNET Sessions:
        Server IP        : 20.1.1.1
        Client IP        : 20.1.1.2
        Client Port      : 58837
```

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 **default** VRF:

```
switch(config)# telnet server vrf default
```

Configuring the Telnet server on the **mgmt** VRF:

```
switch(config)# telnet server vrf mgmt
```

Command History

Release	Modification
10.11	Command introduced on 9300, 1000, 4100i and 8xxx platforms.
10.08.1021	Command introduced on the 6200, 6300, 6400 Switch Series.

Command Information

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

Configuring a layer 2 interface

Procedure

1. Change to the interface configuration context for the interface with the command `interface`.
2. By default, interfaces are layer 3. To create a layer 2 interface, disable routing with the command `no routing`.
3. Set the interface MTU (maximum transmission unit) with the command `mtu`.
4. Review interface configuration settings with the command `show interface`.

Example

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# mtu 1900
```

Configuring a layer 3 interface

Procedure

1. Change to the interface configuration context for the interface with the command **interface**.
2. Interfaces are layer 3 by default. If you previously set the interface to layer 2, then enable routing support with the command **routing**.
3. Assign an IPv4 address with the command **ip address**, or an IPv6 address with the command **ipv6 address**.
4. If required, enable support for layer 3 counters with the command **l3-counters**.
5. If required, set the IP MTU with the command **ip mtu**.
6. Review interface configuration settings with the command **show interface**.

Examples

This example creates the following configuration:

- Configures interface **1/1/1** as a layer 3 interface.
- Defines an IPv4 address of **10.10.20.209** with a 24-bit mask.

```
switch# config
switch(config)# interface 1/1/1
switch(config-if)# ip address 10.10.20.209/24
```

This example creates the following configuration:

- Configures interface **1/1/2** as a layer 3 interface.
- Defines an IPv6 address of **2001:0db8:85a3::8a2e:0370:7334** with a 24-bit mask.
- Enables layer 3 transmit and receive counters.

```
switch# config
switch(config)# interface 1/1/2
switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
switch(config-if)# l3-counters tx
switch(config-if)# l3-counters rx
```

Single source IP address

Certain IP-based protocols used by the switch (such as RADIUS, sFlow, TACACS, and TFTP), use a client-server model in which the client's source IP address uniquely identifies the client in packets sent to the server. By default, the source IP address is defined as the IP address of the outgoing switch interface on which the client is communicating with the server. Since the switch can have multiple routing interfaces, outgoing packets can potentially be sent on different paths at different times. This can result in different source IP addresses being used for a client, which can create a client identification problem on the server. For example, it can be difficult to interpret system logs and accounting data on the server when the same client is associated with multiple IP addresses.

To resolve this issue, you can use the commands `ip source-interface` and `ipv6 source-interface` to define a single source IP address that applies to all supported protocols (RADIUS, sFlow, TACACS, and TFTP), or an individual address for each protocol. This ensures that all traffic sent by a client to a server uses the same IP address.

Priority-based flow control (PFC)

Priority-based flow control (PFC) is defined in the IEEE 802.1Qbb standard. It is used to eliminate packet loss due to congestion on a network link.

For priority-based flow control, care must be taken when configuring quality of service.

1. Configure the global CoS map (`qos cos-map` command) and queue profile (`qos queue-profile` command) before configuring PFC on any interface.
   - Each code point in the CoS Map to be used for PFC must be assigned a unique local-priority value.
   - Each local-priority used for PFC must be the sole local-priority mapped to a queue in the queue profile.
2. CoS map or queue profile changes for non-PFC priorities can be modified without any impact on PFC functionality.
3. All interfaces with PFC enabled must also be configured with `qos trust cos` or `qos trust dscp.`
4. For PFC to function properly with VSX and MCLAG, PFC must be configured on the inter-switch-link.

See also commands flow-control and show interface flow-control.

Refer to the *Quality of Service Guide* for more information about buffering and queuing for flow-controlled traffic.

(Applies to the 8325, 9300, 10000)

On 8325 and 10000 series switches, a maximum of three unique PFC priority combinations can be configured for the entire switch. On 9300 series switches, a maximum of seven unique PFC priority combinations can be configured for the entire switch. Note that ports with a PFC configuration that cannot be applied can still link up, but will not have any flow control. For example, when ports 1 to 4 are configured for PFC priorities 3 and 4, ports 5 to 8 for PFC priority 4, and ports 9 to 12 for PFC priority 5, then any other ports can only be configured for priority combinations of 3, 4, or 5. If a fourth priority combination is configured the following error message will be displayed:

```
The number of unique priority-based flow control (PFC) configuration combinations
cannot be more than 3.
```

With PFC configured for TX, RXTX, or both, PFC cannot be enabled on an interface if the PFC priority is not mapped to a lossless pool. If you attempt to configure a PFC priority on an interface without mapping it to a lossless pool, the switch will display the following message:

```
All TX flow-controlled priorities must first be mapped to a lossless pool using
the 'qos pool' command.
```

Best practices is to configure priority-based flow control (PFC) or link-level flow control RXTX mode and pools only once on a running system. Changing the pool or flow control configuration on a running system will cause brief traffic disruption and packets may be lost in the data flow while the reconfiguration occurs. This may effect one, multiple, or all ports depending on the existing configuration and changes made to it.

(Applies to the 8325, 9300, 10000) Asymmetric PFC

Although PFC is typically symmetric in that it applies to both the receiving (RX) and sending (TX) of PFC pause frames, it can be configured (using the flow-control command) to only respond to received (RX) PFC pause frames or to only send (TX) PFC pause frames. This is referred to as asymmetric PFC. Asymmetric PFC can be useful to implement PFC in only one direction in parts of the network. For example, it could be desirable to have an uplink port that treats arriving traffic as lossless (respecting PFC pause frames) but not transmit PFC pause frames into the spine or core of the network. This capability can be used to deal with the unique requirements of some NICs which require asymmetric PFC configuration to ensure proper behavior.

(Applies to the 8360)

PFC cannot be enabled on an interface that also has a MACsec policy configured. If both PFC and MACsec are configured on an interface, it will remain down until one or the other is removed.

Reboot is required to split or unsplit a port that has had link up with PFC or RXTX enabled. Until reboot, the interface will remain down with a status of `Split in progress` or `Unsplit in progress`.

Configurable flow control buffer thresholds

For the 8325, 9300, and 10000 series switch:

The switch supports the configuration of XOFF limit, XON delta and headroom limit buffer thresholds on flow control enabled interfaces using flow-control buffer commands. QoS buffer configuration using flow-control buffer commands are only applicable to ports or priorities configured for flow-control. If specified for a port or priority not configured for flow-control, the configuration has no effect. QoS buffer configuration for PFC priorities are not applicable to LLFC RXTX ports and vice versa.

QoS buffer configuration for PFC priorities are not applicable to LLFC RXTX ports.

For information on this feature, see the related video on the AirHeads Broadcasting Channel.

XOFF limit

XOFF limit defines the amount of shared buffer space flow-controlled packets allowed to consume before a pause is asserted to the link partner. The lossless buffer limits for traffic arriving on flow control enabled ports or priorities can be optionally configured using one of the following two modes:

- Dynamic XOFF limit: The dynamic limit scales as a function of available buffer resources and is configured by specifying an alpha value in the range between *-7* and *3*. The dynamic limit is based on the currently available free space, multiplied by 2 raised to the power of the specified alpha value. A value less than zero means that the limit is a fraction of the pool free space. For example, *-1* corresponds to half. A value greater than zero means that the limit is a multiple of the free-space size. For example, an alpha value of *1* corresponds to double.

If the user-configured limit is not specified, the default limit of dynamic alpha *1* is configured.

- Static XOFF limit: The static limit sets a fixed size for the XOFF threshold.

XON delta

XON delta defines the offset value below the XOFF limit when a pause is de-asserted to the link partner. The delta value is relative to the XOFF limit and applies to both dynamic and static XOFF limit configurations. When the buffer in-use amount from a source port (LLFC RXTX) or source port with priority (PFC) reaches the XOFF limit, a pause is asserted to the link peer. At this point, the pause will remain asserted until the shared buffer in-use amount by the LLFC RXTX port or priority decreases by the XON delta amount. Once enough packets are transmitted to reduce in-use by this amount, the pause is de-asserted.

It is important to note that the XON delta value will impact the amount of flow control pause frames sent to the link peer and can have a negative impact on performance. A value that is too small can result in many more pause frames sent to the link peer as the buffer in-use amount reaches the XOFF limit, drops slightly, and meets the XON delta, then immediately jumps back to the XOFF limit. Conversely, a value that is too large can result in poor link bandwidth utilization due to insufficient buffered packets as the buffer drains too far before more packets arrive to utilize the link. The default XON Delta value is 12288 bytes.

Headroom size

This value can be explicitly configured by setting the buffer size or implicitly configured by setting the cable length. If both are specified, the buffer size value is used and the cable length is ignored.

Headroom limit

Headroom limit defines the amount of buffer space reserved to absorb any in-flight packets from the time that the XOFF message is transmitted by the local device until the time that the last packet is sent by the link partner and received by the local device. Headroom Limit for an LLFC RXTX port or PFC priority sets a fixed size of headroom pool buffer space for in-flight packets that arrive after XOFF is asserted.

Cable length value

Indirectly adjusts the headroom buffer length on the physical interface. Cable length is one of the delay components that effects traffic round trip time (RTT). Based on IEEE std 802.1Qbb, RTT depends on several delay components such as PFC transmission delay, Interface Delay, Cable Delay and Higher layer delay. Cable length configuration changes the cable delay component of RTT and is used to compute

the headroom buffer length for in-flight packets that arrive after XOFF is asserted. If both headroom buffer limit and cable length are configured, the headroom buffer limit is used and cable length is ignored.

Cable Length Auto

Auto mode will compute the headroom size using the length of the attached cable when known. If the cable length cannot be determined, headroom is computed using the configured cable length or the default length of 350 meters.

Cable Length Default

If none of the commands that adjust the headroom limit are configured, a default cable-length of 350 meters is used to compute the headroom pool limit.

Default buffer thresholds

By default, when the LLFC RXTX or PFC is enabled, the switch uses a dynamic buffer threshold for the XOFF limit, a delta value for XON, and a headroom buffer limit based on 350m cable length.

For many scenarios, these defaults are sufficient to provide good performance without any issues. However, in some situations it is useful to tune the XOFF limit, XON delta, and headroom parameters based on the unique requirements of a particular deployment. In those situations, the buffer tuning capabilities described in this section can be useful to optimize memory usage.

The flow control buffer configurations are optional. If the configurations are not done, defaults are used.

Flow control buffer tasks

The flow control buffer tasks are as follows:

Tasks	Command	Examples

Configuring dynamic XOFF limit	`flow-control buffer priority <PRIORITY>`
	`xoff dynamic <ALPHA>`
	`flow-control buffer llfc`
	`xoff dynamic <ALPHA>`
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer priority 5`
		`xoff dynamic -3`
		
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer llfc`
		`xoff dynamic -3`

Configuring static XOFF limit	`flow-control buffer priority <PRIORITY>`
	`xoff static <LIMIT> kbytes`
	`flow-control buffer llfc`
	`xoff static <LIMIT> kbytes`
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer priority 6`
		`xoff static 128 kbytes`
		
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer llfc`
		`xoff static 128 kbytes`

Tasks	Command	Examples

Configuring XON delta	`flow-control buffer priority <PRIORITY> xon <VALUE> kbytes`
	`flow-control buffer llfc xon <VALUE> kbytes`
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer priority 4 xon 24 kbytes`
		
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer llfc xon 24 kbytes`

Configuring headroom limit	`flow-control buffer priority <PRIORITY> headroom <LIMIT> kbytes`
	`flow-control buffer llfc headroom <LIMIT> kbytes`
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer priority 4 headroom 36 kbytes`
		
		`switch(config)# interface 1/1/1`
		`switch(config-if)# flow-control buffer llfc headroom 36 kbytes`

Flow control and lossless buffering

For the 8325, 9300, and 10000 series switch:

The switch supports IEEE 802.1Q Priority-based Flow Control (PFC). The PFC standard specifies additional frames exchanged between the Ethernet Media Access Controllers (MACs) on both sides of a link to pause and resume transmissions. The goal is to prevent packet loss despite congestion.

Prerequisites

1. A Priority Code Point (PCP) chosen for PFC must not share a local priority with any other PCP in the Class of Service (CoS) map.
2. A local priority mapped to the PCP via the CoS Map must be the only local priority assigned to its queue in the queue profile.

NOTE: These prerequisites should be configured during initial switch provisioning and only changed during maintenance periods where all ports are disabled and the switch is then rebooted.

Requirements for proper lossless buffering:

- Lossless buffering is only supported for single destination (i.e. unicast) traffic. Multi-destination traffic cannot be guaranteed to be lossless.
- All traffic with the specified PCP arriving on PFC-configured ports must be destined for another PFC-configured-port with an egress queue with the same PCP.

- All packets arriving on PFC-configured ports or arriving on non-PFC ports must not be destined for an egress port queue used by PFC traffic with a different PCP.
- If traffic path contains Layer 3 interface then ECN would also need to be added to the configuration.
- The switch has maximum of 3 PFC lossless priorities and does not support PFC below 10 Gbps.

By default, all switch buffering is in one pool shared by all ports called the Lossy pool. Any packet intending to use the Lossy pool can be dropped if the egress port queue is above its limit. Egress queue limits are dynamic based on the amount of free buffers available in the Lossy pool. The TX Drops columns displayed from the *show interface* <*IF-NAME*> command will display the number of drops that have occurred.

All traffic with the specified PCP arriving on PFC-configured ports will share the Lossless or Headroom pools. Any packets using these pools will never be dropped when an egress queue exceeds its limit. All other packets arriving on PFC-configured ports with different PCPs or on non-PFC ports will share the Lossy pool and be subject to dropping when an egress queue is over its limit.

Each PFC-configured port priority is given a limit for the amount of Lossless pool buffering its arriving packets can use. Once the limit is exceeded, the switch will transmit a priority pause frame from the port to stop further packets arriving. Due to link propagation time and processing time on the receiving switch additional packets may be received and stored in the Headroom pool.

When the switch receives a PFC pause frame for the configured PCP the port will cease transmitting further packets from that queue until the timeout specified in the Quanta field has expired or a resume frame is received.

For the 8360 series switch:

The switch supports IEEE 802.1Q Priority-based Flow Control (PFC) and 802.3x Link Level Flow Control (LLFC). These standards specify additional frames exchanged between the Ethernet Media Access Controllers (MACs) on both sides of a link to pause and resume transmissions. The goal is to prevent packet loss despite congestion.

Prerequisites

1. A Priority Code Point (PCP) chosen for PFC must not share a local priority with any other PCP in the Class of Service (CoS) map.

2. A local priority mapped to the PCP via the CoS map must be the only local priority assigned to its queue in the queue profile.

NOTE: These prerequisites should be configured during initial switch provisioning and only changed during maintenance periods where all ports are disabled.

Requirements for proper lossless buffering

- Lossless buffering is only supported for single-destination (i.e. unicast) traffic. Multi-destination traffic is not guaranteed to be lossless.
- All arriving flow-controlled traffic must only be transmitted by flow-controlled ports or port queue(s):
  - For LLFC-operating ports all arriving traffic must be destined for another LLFC port.
  - For PFC-enabled ports all arriving packets with the configured PCP must be destined for another PFC-enabled port queue with the same PCP.
- All arriving non-flow-controlled traffic must only be transmitted by non-flow-controlled ports or port queue(s).

- For traffic arriving on non-LLFC ports and on PFC ports with different PCPs, packets must not be destined to be transmitted out an LLFC-operating port or a PFC-enabled port queue.
- PFC cannot be used on MACsec configured ports
- The switch can support 2 PCPs for per port

By default, all switch buffering is in one pool shared by all ports called the Lossy pool. Any packet attempting to use the Lossy pool can be dropped if the egress port queue is above its limit. Egress port queues have a limit of 2 MB divided equally among the number of queues in the applied queue profile. For example, when using the 8-queue factory-default profile the egress queue limit is 256 KB. The TX Drops columns of *show interface <IF-NAME>* command will display the number of drops that may have occurred.

Flow Control reconfigures buffering. After the first interface is configured for PFC the switch will segregate buffering into multiple pools:

- Lossy Pool (default)
- Lossless Pool
- Headroom Pool

Buffers are moved from the Lossy to the Lossless and Headroom pools depending on the number and maximum possible speed of the ports on the switch model. The Headroom pool size assumes that all port cables are 300 meters in length.

NOTE: Using slower port speeds or different cable lengths will not change the pool allocations.

All traffic with the specified PCP arriving on PFC-configured ports or on an LLFC-operating port will share the Lossless and Headroom pools. Any packets stored in these pools will never be dropped if an egress queue exceeds its limit. All other packets arriving on non-flow-control ports, or on PFC-enabled port(s) with different PCPs will share the Lossy pool and be subject to drops when an egress queue exceeds its limit.

Each LLFC port and each PFC-port priority has a limited amount of Lossless pool buffer space that arriving packets are allowed to use. Once the limit is exceeded the switch will transmit a pause frame out the port to stop further packets from arriving. Due to link propagation time and processing time on the receiving switch, additional packets in flight may be received and will share the Headroom pool. The switch will periodically transmit priority pause frames until none of packets on the arriving port are in the Headroom pool and half of the port's shared buffer below the pause limit is available.

When the switch receives a PFC pause frame for the configured PCP, the port will cease transmitting further packets from that queue until the timeout specified in the Quanta field has expired or a resume frame is received.

Forward error correction

Forward error correction (FEC) is used to control errors in transmissions where the source sends redundant data and the destination only recognizes the data portion that contains no apparent errors. FEC does not require a handshake between the source and destination at the cost of a higher forward channel bandwidth. It is therefore best used in scenarios where re-transmissions are costly or impossible, such as using multicast one-way communication.

Unsupported transceiver support

Transceiver products (optical, DAC, AOCs) that are listed as supported by a switch model are detailed in the *Transceiver Guide*. Transceiver products that are not listed, are considered unsupported; this would include transceivers that are:

- Non-HPE Aruba Networking branded products
- HPE branded products that were designed for non-AOS-CX switch models (e.g. Comware)
- HPE branded products designated for use in HPE Compute Servers or Storage
- Transceivers originally designated for use in HPE Aruba Networking WLAN controllers or former Mobility Access Switch (MAS) products
- End-of-life HPE Aruba Networking Transceivers

The unsupported transceiver mode (UT-mode) is designed to allow the possible use of these unsupported products. Not all unsupported products can be recognized and enabled; they may be unable to be identified (do not follow the proper MSA standards for identification). These unsupported transceiver products are enabled only on a best-effort basis and there are no guarantees implied for their continued operation.

This feature is enabled by default. A periodic system log will be generated by default at an interval of 24 hours listing the ports on which unsupported transceivers are present. The log interval is configurable and can be disabled by setting the log-interval to **none**.

Configuring an interface persona

A persona is a template interface. It is a mechanism intended to ease the process of configuring one or multiple interfaces that behave in the same manner. For example, a persona could be an uplink interface with a well-known collection of VLANs to which it belongs. Instead of manually configuring each interface one-by-one, the persona collects the common configuration settings and allows them to be applied on the interface or a collection of interfaces.

Persona configuration is similar to configuring other interfaces. Most of the commands in the interface context are available. Because of the nature of the commands, several of them do not apply to the persona (for example, applying the same IP address configuration to several ports) and have been removed from the available list.

Configuration AAA and port-access commands is not supported within the interface context when configuring a persona:

```
switch(config)# interface persona access
switch(config-if)#port-access <command>
switch(config-if)#aaa <command>
```

In addition, the following commands are not supported:

```
aaa authentication port-access dot1x authenticator macsec
aaa authentication port-access dot1x supplicant
aaa authentication port-access dot1x authenticator mka cak-length
arp ipv4 <IPV4_ADDR> mac <MAC_ADDR>
downshift-enable
energy-efficient-ethernet
error-control { auto | none | base-r-fec | rs-fec }
ip bootp-gateway <IPV4-ADDR>
ip forward-protocol udp <IPV4-ADDR> {<PORT-NUM> | <PROTOCOL>}
ip helper-address <IPV4-ADDR> [vrf <VRF-NAME>]
ip igmp router-alert-check [enable | disable]
ip igmp snooping [auto vlan <VLAN-LIST>]
ip igmp snooping [blocked vlan <VLAN-LIST>]
ip igmp snooping [fastleave vlan <VLAN-LIST>]
ip igmp snooping [forced-fastleave vlan <VLAN-LIST>]
ip igmp snooping [forward vlan <VLAN-LIST>]
```

```
ip ospf <PROCESS-ID> area <AREA-ID>
ip ospf passive
ip rip <PROCESS-ID> {all-ip | ip-address}
ip rip all-ip disable
ip rip all-ip enable
ip rip all-ip receive disable
ip rip all-ip send disable
ipv6 helper-address multicast {all-dhcp-servers | <MULTICAST-IPV6-ADDR>} egress <PORT-
NUM>
ipv6 mld snooping [auto vlan <VLAN-LIST>]
ipv6 mld snooping [blocked vlan <VLAN-LIST>]
ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
ipv6 mld snooping [forced-fastleave vlan <VLAN-LIST>]
ipv6 mld snooping [forward vlan <VLAN-LIST>]
ipv6 neighbor <IPV6-ADDR> mac <MAC-ADDR>
ipv6 ospfv3 <PROCESS-ID> area <AREA-ID>
ipv6 ospfv3 passive
ipv6 ripng <PROCESS-ID>
lacp port-id <PORT-ID>
lacp port-priority <PORT-PRIORITY>
lag <ID>
link-poe
lldp dot3 eee
lldp dot3 poe
lldp med poe
lldp med poe [priority-override]
persona {access | uplink | custom <PERSONA-NAME>} [copy | attach]
port-access port-security sticky-learn mac-address
power-over-ethernet
power-over-ethernet allocate-by {usage | class}
power-over-ethernet assigned-class {3 | 4 | 6 | 8}
power-over-ethernet pd-class-override
power-over-ethernet power-pairs {alt-a|alt-a-and-alt-b}
power-over-ethernet pre-std-detect
power-over-ethernet priority {critical|high|low}
ptp lag-role {primary | secondary}
spanning-tree cost <PORT-COST>
spanning-tree instance <INSTANCE-ID> cost <PORT-COST>
spanning-tree instance <INSTANCE-ID> port-priority <PRIORITY-MULTIPLIER>
spanning-tree port-priority <PRIORITY-MULTIPLIER>
spanning-tree vlan <A:1-4094> cost <0-200000000>
spanning-tree vlan <A:1-4094> port-priority <0-15>
split [confirm]
track by <OBJECT-ID>
vsx-sync {access-lists | qos | rate-limits | vlans | policies | irdp}
```

Modes

There are three supported modes:

1. Copy—The **copy** mode is a one-step configuration that copies the persona configuration to an interface. Further changes to the persona will not be applied to the interfaces using that mode.

2. Attach—Unlike the **copy** mode, besides applying the configuration to the interface immediately, the **attach** mode also follows the persona configuration. It means that the subsequent changes to the persona will be applied to the interfaces attached to it.

3. Label—The **label** mode follows the interface persona configuration. The two exceptions are **copy** and **attach** modes. The **label** mode classifies the purpose of an interface and maintains functionality without requiring a persona to exist.

Predefined and custom persona names

There are two predefined interface persona names:

- uplink
- access

These names have no predefined configuration. To use them, they must be manually configured as needed. You can also create personas with a custom name. These custom personas can be created and configured in the same manner as the predefined ones. The only difference is the command used to apply them to the interface. The procedure below provides the details.

Creating and configuring an interface persona

Follow these steps to create and configure an interface persona:

1. Create the interface **persona** with the command **interface persona <*PERSONA-NAME*>**.
2. Set the interface configuration as any other physical interface.
3. Review the configuration with the command **show running-configuration current-context**.
4. Switch to an interface context with the command **interface <*PORT*>**.
5. Apply the persona configuration to the interface and set the mode with the command **persona custom <PERSONA-NAME> <mode>**. Note that **<*custom*>** is listed among the three arguments required for configuration.

For information on this feature, see the related video on the AirHeads Broadcasting Channel.

All interface configurations related to Device-Profile are supported persona interface.

Examples

To copy a predefined persona name configuration to an interface:

1. Configure 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. Apply the configuration with **copy** mode:

```
switch(config)# interface 1/1/1
switch(config-if)# persona uplink copy
switch(config-if)# exit
```

To attach a custom persona name to several interfaces simultaneously:

1. Configure the interface persona:

```
switch(config)# interface persona mytemplate
switch(config-if)# no shutdown
switch(config-if)# vrf attach upstream
```

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

2. Apply the configuration with **attach** mode:

```
switch(config)# interface 1/1/1-1/1/24
switch(config-if)# persona custom mytemplate attach
switch(config-if)# exit
```

To label a custom persona name to an interface:

1. Apply the configuration with **label** mode:

```
switch(config)# interface 1/1/1
switch(config-if)# persona custom mypersona
switch(config-if)# exit
```

```
link-poe
lldp dot3 eee
lldp dot3 poe
lldp med poe
lldp med poe [priority-override]
persona {access | uplink | custom <PERSONA-NAME>} [copy | attach]
port-access port-security sticky-learn mac-address
power-over-ethernet
power-over-ethernet allocate-by {usage | class}
power-over-ethernet assigned-class {3 | 4 | 6 | 8}
power-over-ethernet pd-class-override
power-over-ethernet power-pairs {alt-a|alt-a-and-alt-b}
power-over-ethernet pre-std-detect
power-over-ethernet priority {critical|high|low}
ptp lag-role {primary | secondary}
spanning-tree cost <PORT-COST>
spanning-tree instance <INSTANCE-ID> cost <PORT-COST>
spanning-tree instance <INSTANCE-ID> port-priority <PRIORITY-MULTIPLIER>
spanning-tree port-priority <PRIORITY-MULTIPLIER>
spanning-tree vlan <A:1-4094> cost <0-200000000>
spanning-tree vlan <A:1-4094> port-priority <0-15>
split [confirm]
track by <OBJECT-ID>
vsx-sync {access-lists | qos | rate-limits | vlans | policies | irdp}
```

Modes

There are three supported modes:

1. Copy—The **copy** mode is a one-step configuration that copies the persona configuration to an interface. Further changes to the persona will not be applied to the interfaces using that mode.

2. Attach—Unlike the **copy** mode, besides applying the configuration to the interface immediately, the **attach** mode also follows the persona configuration. It means that the subsequent changes to the persona will be applied to the interfaces attached to it.

3. Label—The **label** mode follows the interface persona configuration. The two exceptions are **copy** and **attach** modes. The **label** mode classifies the purpose of an interface and maintains functionality without requiring a persona to exist.

Predefined and custom persona names

There are two predefined interface persona names:

- uplink
- access

These names have no predefined configuration. To use them, they must be manually configured as needed. You can also create personas with a custom name. These custom personas can be created and configured in the same manner as the predefined ones. The only difference is the command used to apply them to the interface. The procedure below provides the details.

Creating and configuring an interface persona

Follow these steps to create and configure an interface persona:

1. Create the interface **persona** with the command **interface persona <*PERSONA-NAME*>**.
2. Set the interface configuration as any other physical interface.
3. Review the configuration with the command **show running-configuration current-context**.
4. Switch to an interface context with the command **interface <*PORT*>**.
5. Apply the persona configuration to the interface and set the mode with the command **persona custom <PERSONA-NAME> <mode>**. Note that **<*custom*>** is listed among the three arguments required for configuration.

For information on this feature, see the related video on the AirHeads Broadcasting Channel.

All interface configurations related to Device-Profile are supported persona interface.

Examples

To copy a predefined persona name configuration to an interface:

1. Configure 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. Apply the configuration with **copy** mode:

```
switch(config)# interface 1/1/1
switch(config-if)# persona uplink copy
switch(config-if)# exit
```

To attach a custom persona name to several interfaces simultaneously:

1. Configure the interface persona:

```
switch(config)# interface persona mytemplate
switch(config-if)# no shutdown
switch(config-if)# vrf attach upstream
switch(config-if)# exit
```

2. Apply the configuration with **attach** mode:

```
switch(config)# interface 1/1/1-1/1/24
switch(config-if)# persona custom mytemplate attach
switch(config-if)# exit
```

To label a custom persona name to an interface:

1. Apply the configuration with **label** mode:

```
switch(config)# interface 1/1/1
switch(config-if)# persona custom mypersona
switch(config-if)# exit
```

Monitor mode

Monitor mode displays interface statistics in real time, updating frequently. The update interval varies by product, number of visible ports, and display options in use. View the current update interval in the help menu.

Formatting options can be supplied either at command launch or while monitor mode is active. Press `?` to see the available formatting options available in the current command context. Exit the help menu with `q`.

Monitor mode detects terminal size to adjust the number of interfaces and statistics viewable on screen. Additional interfaces or statistics columns can be viewed with the navigation keys: Arrow keys, PageUp, PageDown, Home, and End. Serial console does not automatically detect terminal setting changes, resulting in unexpected output. Recommended recovery steps are to exit and restart.

Monitor mode refreshes data automatically until exited with `q`.

Interface commands

allow-unsupported-transceiver

```
allow-unsupported-transceiver [confirm | log-interval {none | <INTERVAL>}]
no allow-unsupported-transceiver
```

Description

Allows unsupported transceivers to be enabled or establish connections. Transceivers with speeds up to 100G are enabled by this command.

- The following models will enable unsupported transceivers for speeds up to 100G when running AOS-CX 10.09.0001 or later:
  - 8325 (Models 48Y8C and 32C)
  - 8360 (Models 48Y6C, 32Y4C, 16Y2C, 48XT4C, 24XF2C and 12C)
  - 9300/9300S Series Switches
  - 10000 Series Switches
- The 8320 Series Switches will enable unsupported transceivers for speeds up to 40G when running AOS-CX 10.10 or later.

This command is enabled by default, allowing the use of third party transceiver products without adding the command in the configuration. Disabling this command with the **no** form will now disable the command in the running and stored configurations.

The **no** form of this command disallows using unsupported transceivers.

Parameter	Description
`confirm`	Specifies that unsupported transceiver warnings are to be automatically confirmed.
`log-interval none`	Disables unsupported transceiver logging.
`log-interval <INTERVAL>`	Sets the unsupported transceiver logging interval in minutes. Default: 1440 minutes. Range: 1440 to 10080 minutes.

Usage

When none of the parameters are specified it will display a warning message to accept the warranty terms. With **confirm** option the warning message is displayed but the user is not prompted to **(y/n)** answering. Warranty terms must be agreed to as part of enablement and the support is on best effort basis.

Examples

Allowing unsupported transceivers with follow-up confirmation:

```
switch(config)# allow-unsupported-transceiver
Warning: The use of unsupported transceivers, DACs, and AOCs is at your
own risk and may void support and warranty. Please see HPE Warranty terms
and conditions.

Do you agree and do you want to continue (y/n)? y
```

Allowing unsupported transceivers with confirmation in command syntax:

```
switch(config)# allow-unsupported-transceiver confirm
Warning: The use of unsupported transceivers, DACs, and AOCs is at your
own risk and may void support and warranty. Please see HPE Warranty terms
and conditions.
```

Configuring unsupported transceiver logging with an interval of every 48 hours:

```
switch(config)# allow-unsupported-transceiver log-interval 2880
```

Disabling unsupported transceiver logging:

```
switch(config)# allow-unsupported-transceiver log-interval none
```

Disallowing unsupported transceivers with follow-up confirmation:

```
switch(config)# no allow-unsupported-transceivers
Warning: Unsupported transceivers, DACs, and AOCs will be disabled,
which could impact network connectivity. Use 'show allow-unsupported-transceiver'
to identify unsupported transceivers, DACs, and AOCs.

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)#
```

Command History

Release	Modification
10.10	Up to 100G support enabled for unsupported transceivers on 8320 (Up to 40G) series switches in UT mode.
10.09	Up to 100G support enabled for unsupported transceivers on 8325, 8360 and 10000 series switches in UT mode.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	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.

Parameter	Description
	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
```

Command History

Release	Modification
10.07 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
```

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.

diag dsm console

diag dsm console *<SLOT-ID>*

Description

Provides access to the operator console of the attached distributed services module. From this console, operator commands can be run. Exiting the console returns the user back to CLI. This is intended for diagnostic purposes only.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.

Examples

Accessing the DSM console **1/1**:

```
switch(config)# diagnostic
switch(config)# diag dsm console 1/1
Distributed Services module 1/1 is ready
IP 169.254.13.1
# pwd
/root
# exit
Connection to 169.254.13.1 closed.
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

error-control

```
error-control {auto | none | base-r-fec | rs-fec}
no error-control {auto | none | base-r-fec | rs-fec}
```

Description

Configures the forward error correction (FEC) mode to use for an interface. When not configured, the system will automatically select the FEC mode based on the installed transceiver. In most cases, the standard FEC mode will work best, but certain link partners may require a non-standard mode.

The **no** and **auto** forms of this command configure the interface to automatically use the standard FEC mode of the currently installed transceiver.

FEC configuration only applies to transceivers, DACs, or AOCs running at 25G or 100G. 100G DACs are a special case. They can only set FEC to none when auto-negotiation is disabled through the **speed override** command. The default for the installed transceiver is used in all other cases.

Transceivers for which FEC is auto-negotiated will request the mode configured by this command, but may resolve to a different mode. The applied FEC mode is displayed as a commented line in the configuration shown with the **show run** command. It is also displayed with **show interface** command.

Parameter	Description
`auto`	Use the transceiver default.
`none`	Do not use any FEC.
`base-r-fec`	Use IEEE BASE-R (Firecode) FEC.
`rs-fec`	Use IEEE RS (Reed-Solomon) FEC.

Command History

Release	Modification
10.08.1021	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P	`config-if`	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8360 9300 9300S 10000		

flow-control

On the 8320:

```
flow-control rx
no flow-control rx
```

On the 8325:

```
flow-control {rx | rxtx [pool <POOL-NUM>]}
no flow-control {rx | rxtx [pool <POOL-NUM>]}
flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
no flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
```

Note: Up to three priority lists in the same command are supported, one each for `rxtx`, `rx`, and `tx`.

On the 8100, 8360:

```
flow-control {rx | rxtx}
no flow-control {rx | rxtx}
flow-control priority rxtx <PRIORITY-LIST>
no flow-control priority rxtx <PRIORITY-LIST>
```

On the 9300/9300S:

```
flow-control {rx | rxtx [pool <POOL-NUM>]}
no flow-control {rx | rxtx [pool <POOL-NUM>]}
flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
no flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
```

Note: Up to three priority lists in the same command are supported, one each for `rxtx`, `rx`, and `tx`.

On the 10000:

```
flow-control {rx | rxtx [pool <POOL-NUM>]}
no flow-control {rx | rxtx [pool <POOL-NUM>]}
flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
no flow-control priority {rxtx <PRIORITY-LIST> | rx <PRIORITY-LIST> | tx <PRIORITY-LIST>}
...
```

Note: Up to three priority lists in the same command are supported, one each for `rxtx`, `rx`, and `tx`.

Description

On the 8320, **flow-control** enables negotiation of receive flow control on the current interface. The switch advertises RX support to the link partner.

On the 8100, 8325, 8360, 9300/9300S, and 10000, **flow-control** enables negotiation of either receive-only flow control or both receive and transmit flow control on the current interface. The switch advertises either RX or RXTX support to the link partner. The final configuration is determined based on the capabilities of both partners.

On the 8100, 8325, 8360, 9300/9300S, and 10000, **flow-control priority** enables priority-based flow control (PFC). Multiple priorities are supported. Bidirectional (symmetric) PFC is configured with parameter **priority rxtx**. Unidirectional (asymmetric) PFC is configured with either parameter **priority rx** or **priority tx**.

On the 8100, 8325, 8360, 9300/9300S, and 10000, when configuring PFC for multiple priority levels, the complete list of priorities must be specified in a single command. Priorities cannot be added or subtracted using separate commands.

Each invocation of this command replaces the previous configuration.

The **no** form of these commands disables any configured flow control on the selected interface.

Parameter	Description
`rx`	Enables the ability to cease and resume transmission when receiving IEEE 802.3x LLFC pause frames on this interface.
`rxtx`	(Applies to the 8100 and 8360.) Enables the ability to honor received and to transmit IEEE 802.3x LLFC pause frames to the remote device.
`rxtx [pool <POOL-NUM>]`	(Applies to the 8325, 9300/9300S, 10000.) **`rxtx`** enables the ability to honor received and to transmit IEEE 802.3x LLFC pause frames to the remote device. **`pool <POOL-NUM>`** optionally selects the number of the lossless pool used for buffering packets arriving on this interface. Default: 1. Range: 1 to 3.
`priority rxtx`	(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enables the ability to honor received and to transmit IEEE 802.1Qbb PFC pause frames on the interface for the configured packet priority.
`priority rx`	(Applies to the 8325, 9300/9300S, 10000.) Enables the ability to honor received IEEE 802.1Qbb PFC pause frames on the interface for the configured packet priorities. This can be useful for implementing asymmetric PFC when it is desired to configure this only in the receive direction.
`priority tx`	(Applies to the 8325, 9300/9300S, 10000.) Enables the ability to transmit IEEE 802.1Qbb PFC pause frames on the interface for the configured packet priorities. This can be useful for implementing asymmetric PFC when it is desired to configure this only in the transmit direction.
<PRIORITY-LIST>	(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Specifies a comma-separated list of packet priorities for which PFC will operate. Range: 0 to 7. Up to seven priorities (two on the 8100 and 8360) can be specified in the list.

Usage (flow control)

- For interfaces that auto-negotiate, link-level flow control is subject to negotiation, plus speed and other parameters. Both ends of the link must negotiate the same flow control mode for it to be applied.
- For interfaces that do not auto-negotiate, the configured link-level flow control mode is always applied and the user is responsible for ensuring that both ends of the link are configured for the same mode.
- All members of a LAG must have the same flow control configuration.

- Lossless flow control is only supported for single destination unicast traffic. Replicated traffic (for example, broadcast, multicast, mirroring) cannot be guaranteed to be lossless.
- Lossless behavior is not supported when operating in a VSF stack configuration.

Usage (priority-based flow control (PFC)) (Not applicable to the 8320)

- PFC will only operate correctly between interfaces with the same priority configuration. Traffic flow will not be lossless between interfaces with different priorities or between interfaces where one has PFC enabled and the other does not.
- On the 8325, 9300/9300S, and 10000, PFC takes effect after the configuration is saved and the switch is restarted.
- On the 8325, 9300/9300S, and 10000, lossless pools must be created before configuring flow control on any interface. For PFC (when the PFC mode includes TX), any priority to be configured for PFC must be mapped to a lossless pool before it can be enabled for PFC. For link-level flow control, lossless pool 1 will be used by default if no pool is specified when enabling flow control on the interface. If a pool is specified when enabling flow control on an interface, the specified pool must be created first before enabling flow control.
- Any queue used by protocol or control traffic must not be configured for lossless behavior. Routing protocols and VSX-synchronization messages use local-priority 7, therefore the CoS priority mapped to local-priority 7 should not be used in any lossless configuration.

  For example, in a default configuration, the CoS map assigns local-priority 7 to packets arriving with VLAN priority 7. This means that lossless pools should not be configured to use priority 7, and that any `flow-control priority` mode should not be configured on priority 7, since that VLAN priority maps to local-priority 7.
- On the 8325, 9300/9300S, and 10000, whatever lossless pool(s) will be used for link-level flow control must be created before configuring link-level flow control RXTX mode on any interface. Otherwise, a message similar to the following will be displayed:

  ```
  Lossless pool 1 must be configured using the 'qos pool' command before enabling
  RXTX flow control.
  ```

- On the 8325, 9300/9300S, and 10000, link-level flow control RXTX mode is not subject to auto-negotiation. It is recommended to configure PFC or link-level flow control RXTX mode and pools only once on a running system. Changing the pool or flow control configuration on a running system will cause a brief disruption in traffic. The reconfiguration also results in packet loss in the data flow. This may affect one, multiple, or all ports depending on the existing configuration and changes made to it.
- On the 8360, PFC takes effect immediately after configuration.
- On the 8360 JL720A, PFC is not supported on any link speed below 10 Gbps.

On the 8325, 9300/9300S, and 10000:

You can only apply three unique combinations of PFC priority configuration across all ports of a switch.

For example:

```
flow-control priority 3
flow-control priority 4,5
flow-control priority 4
```

The first three unique combinations configured across all ports sorted in numerical order are accepted and applied. If you attempt to configure a fourth unique priority combination, the following error message is displayed:

```
The number of unique priority-based flow control (PFC) configuration combinations
cannot be more than 3.
```

Note that ports with a PFC configuration that cannot be applied can still link up but they will not have any flow control.

Examples

Enabling support for RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control rx
```

Disabling support for RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control rx
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control txrx
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Disabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control txrx
```

(Applies to the 8325, 9300/9300S, 10000.) Enabling support for RXTX flow control with pool setting:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control rxtx pool 2
```

(Applies to the 8325, 9300/9300S, 10000.) Disabling support for RXTX with pool setting:

```
switch(config)# interface 1/1/1
```

```
switch(config-if)# no flow-control rxtx pool 2
```

(Applies to the 8325, 9300/9300S, 10000.) Enabling support for priority RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control priority rx 3,4
```

(Applies to the 8325, 9300/9300S, 10000.) Disabling support for priority RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control priority rx 3,4
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enabling support for priority RXTX and RX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control priority rxtx 3 rx 1,2,4,5,6
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Disabling support for priority RXTX and RX flow control:

(Applies to the 8325, 9300/9300S, 10000.) Enabling support for priority TX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control priority tx 3,4
```

(Applies to the 8325, 9300/9300S, 10000.) Disabling support for priority TX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control priority tx 3,4
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Enabling support for priority RXTX, RX, and TX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control priority rxtx 3 rx 1,2,4 tx 5,6
```

(Applies to the 8100, 8325, 8360, 9300/9300S, 10000.) Disabling support for priority RXTX, RX, and TX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control priority rxtx 3 rx 1,2,4 tx 5,6
```

Command History

Release	Modification
10.10	Adjusted the priority syntax. Added separate RX and TX configuration for asymmetric PFC. Added the pool parameter.
10.09	Support for `rxtx` added to 8325 Switch Series.
10.08	Command enhanced to configure two PFC priorities.
10.07 or earlier	--

Command Information

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

flow-control buffer headroom

```
flow-control buffer priority <PRIORITY> headroom <LIMIT> kbytes
flow-control buffer llfc headroom <LIMIT> kbytes
no flow-control buffer priority <PRIORITY> headroom <LIMIT> kbytes
no flow-control buffer llfc headroom  <LIMIT> kbytes
```

Description

Allows user configuration of per-priority or LLFC RXTX headroom limit on a physical interface.

The **no** form of the command resets the limit to the default value.

Parameter	Description
`priority <PRIORITY>`	Configures buffer parameters for priority flow control. Range: 0 to 7.
`llfc`	Configures buffer parameters for link-level flow control.
`headroom <LIMIT>`	Specifies the maximum amount of headroom pool buffer space that is allowed to be used for in-flight packets that arrive after flow-control XOFF is asserted. Range: 18 to 10240 kilobytes.

Examples

Configuring a headroom limit of 36 kbytes for PFC priority 4 traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 4 headroom 36 kbytes
```

Configuring a headroom limit of 36 kbytes for LLFC RXTX traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc headroom 36 kbytes
```

Resetting the headroom limit to default value:

```
switch(config)# interface 1/1/1
witch(config-if)#  flow-control buffer priority 4 headroom 36 kbytes
```

Command History

Release	Modification
10.11	Added support for 9300 series switches.
10.10	Command Introduced.

Command Information

Platforms	Command context	Authority
8325 9300 10000	config-if	Administrators or local user group members with execution rights for this command.

flow-control buffer xoff dynamic

```
flow-control buffer priority <PRIORITY> xoff dynamic <ALPHA>
flow-control buffer llfc xoff dynamic <ALPHA>
no flow-control buffer priority <PRIORITY> xoff dynamic <ALPHA>
no flow-control buffer llfc xoff dynamic <ALPHA>
```

Description

Allows user configuration of per-priority or LLFC RXTX dynamic XOFF limits on a physical interface.

The **no** form of the command resets the threshold to the default value.

Parameter	Description
priority *<PRIORITY>*	Configures buffer parameters for priority flow control. Range: 0 to 7.
llfc	Configures buffer parameters for link-level flow control.
<ALPHA>	Specifies the scale factor used to compute the instantaneous buffer limit based on the instantaneous free space. Range: -7 to 3.

Examples

Configuring the dynamic XOFF limit of *-3* for ingress PFC priority *5* traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 5 xoff dynamic -3
```

Configuring the dynamic XOFF limit of *-3* for ingress traffic on an LLFC RXTX port:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc xoff dynamic -3
```

Resetting the xoff dynamic limit to the default:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer priority 5 xoff dynamic
```

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer llfc xoff dynamic
```

Command History

Release	Modification
10.11	Added support for 9300 series switches.
10.10	Command Introduced.

Command Information

Platforms	Command context	Authority
8325 9300 10000	`config-if`	Administrators or local user group members with execution rights for this command.

flow-control buffer xoff static

```
flow-control buffer priority <PRIORITY> xoff static <LIMIT> kbytes
flow-control buffer llfc xoff static <LIMIT> kbytes
no flow-control buffer priority <PRIORITY> xoff static <LIMIT> kbytes
no flow-control buffer llfc xoff static <LIMIT> kbytes
```

Description

Allows user configuration of per-priority or LLFC RXTX static XOFF limits on a physical interface.

The **no** form resets the threshold to the default value.

Parameter	Description
`priority <PRIORITY>`	Configures buffer parameters for priority flow control. Range: 0 to 7.
`llfc`	Configures buffer parameters for link-level flow control.
<LIMIT>	Specifies the absolute limit programmed for the port or priority. When the in-use amount reaches this limit, the XOFF is asserted. Range: 36 to 20000 kilobytes on 8325 and 10000 series switches. Range: 36 to 40000 kilobytes on 9300/9300S series switches.

Examples

Configuring the XOFF static limit of 128 kbytes for PFC priority 6 traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 6 xoff static 128 kbytes
```

Configuring the XOFF static limit of 128 kbytes for LLFC RXTX traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer llfc xoff static 128 kbytes
```

Resetting the xoff static limit to the default:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer priority 6 xoff static
```

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer llfc xoff static
```

Command History

Release	Modification
10.11	Added support for 9300 series switches.
10.10	Command Introduced.

Command Information

Platforms	Command context	Authority
8325 9300 10000	config-if	Administrators or local user group members with execution rights for this command.

flow-control buffer xon

```
flow-control buffer priority <PRIORITY> xon <VALUE> kbytes
flow-control buffer llfc xon <VALUE> kbytes
no flow-control buffer priority <PRIORITY> xon <VALUE> kbytes
no flow-control buffer llfc xon <VALUE> kbytes
```

Description

Allows user configuration of per-priority or LLFC RXTX dynamic XON delta on a physical interface.

The **no** form of the command resets the XON delta to the default value.

Parameter	Description
priority <*PRIORITY*>	Configures buffer parameters for priority flow control. Range: 0 to 7.

Parameter	Description
`llfc`	Configures buffer parameters for link-level flow control.
<VALUE>	Specifies the offset value below the XOFF limit where XON is asserted and packet transmission resumes. Range: 1 to 20000 kilobytes on 8325 and 10000 series switches. Range: 1 to 40000 kilobytes on 9300/9300S series switches.

Examples

Configuring the XON delta of 24 kbytes for PFC priority 4 traffic:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control buffer priority 4 xon 24 kbytes
```

Configuring the XON delta of 24 kbytes for LLFC RXTX traffic:

```
switch(config)# interface 1/1/1

switch(config-if)# flow-control buffer llfc xon 24 kbytes
```

Resetting the xon delta to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer priority 4 xon 24 kbytes
```

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control buffer llfc xon 24 kbytes
```

Command History

Release	Modification
10.11	Added support for 9300 series switches.
10.10	Command Introduced.

Command Information

Platforms	Command context	Authority
8325 9300 10000	`config-if`	Administrators or local user group members with execution rights for this command.

flow-control watchdog

```
flow-control watchdog
no flow-control watchdog
```

Description

Enables flow control watchdog on a physical interface.

When an excessive amount of lossless traffic stops transmitting, problematic lossless buffer congestion occurs throughout the network. To prevent the situation, egress lossless queues are monitored to detect when no transmissions have occurred for a globally specified detection timeout. When the condition is detected, the flow control watchdog triggers on the affected queue resulting in the following actions:

- The watchdog timeout counter on the interface is incremented.
- All packets occupying the affected queue are discarded.
- New packet arrivals destined for the affected queue are discarded.

After the configured resume interval has elapsed since the trigger, the queue is returned to normal operation.

The **no** form of this command disables flow control watchdog on a physical interface.

Flow control watchdog is only supported on interfaces configured with PFC. Link-level flow control is not compatible with flow control watchdog.

When flow control watchdog is enabled, it is active on all lossless queues of the port.

To determine whether the flow control watchdog is enabled on an interface, or to see the number of times the watchdog has been triggered, use the **show interface flow-control** command.

The detection and resume intervals must be configured from the global configuration context.

Examples

Enabling flow control watch on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control watchdog
```

Disabling flow control watch on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control watchdog
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8325 8325H 8325P 9300	config-if	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
9300S 10000		

flow-control watchdog timeout resume

```
flow-control watchdog timeout <MILLISECONDS> resume <MILLISECONDS>
no flow-control watchdog timeout <MILLISECONDS> resume <MILLISECONDS>
```

Description

Configures global flow control watchdog parameters, detection time and resume time. The parameters are applied to all interfaces that have flow control watchdog enabled with command **flow-control watchdog**.

The **no** form of this command clears the global configuration parameters for flow control watchdog, restoring timeout and resume time to the platform defaults.

Flow control watchdog must be enabled on specified interfaces.

The configured timing parameters are rounded to what the hardware supports. Use command **show flow control** to show the applied values.

Using fault monitor, an interface can be configured with additional actions such as **notify** or **notify-and-disable** when flow control watchdog triggers exceed the configured threshold. See *Excessive flow control watchdog triggers* in the *Fault monitor* section of the Security Guide (version 10.12 or higher) for your switch model.

Parameter	Description
`timeout <MILLISECONDS>`	Specifies the amount of time in milliseconds, that a queue must be paused for watchdog to trigger. Range: 10 to 1500 milliseconds. Default: 100 milliseconds.
`resume <MILLISECONDS>`	Specifies the duration of time in milliseconds, that a queue remains in the triggered state. Range: 1 to 100000 milliseconds. Default: 100 milliseconds.

Examples

Configuring flow control watchdog global parameters:

```
switch(config)# flow-control watchdog timeout 100 resume 60
```

Removing flow control watchdog global parameters:

```
switch(config)# no flow-control watchdog timeout 100 resume 60
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
8325 8325H 8325P 9300 9300S 10000	`config`	Administrators or local user group members with execution rights for this command.

interface

`interface <PORT-NUM>`

Description

Switches to the **config-if** context for a physical port. This is where you define the configuration settings for the logical interface associated with the physical port.

Parameter	Description
<PORT-NUM>	Specifies a physical port number. Format: **member/slot/port**.

Examples

Configuring an interface:

```
switch(config)# interface 1/1/1
switch(config-if)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

interface loopback

`interface loopback <ID>`
`no interface loopback <ID>`

Description

Creates a loopback interface and changes to the **config-loopback-if** context. Loopback interfaces are layer 3.

The **no** form of this command deletes a loopback interface.

Parameter	Description
<INSTANCE>	Specifies the loopback interface ID. Range: 1 to 256

Examples

```
switch# config
switch(config)# interface loopback 1
switch(config-loopback-if)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config	Administrators or local user group members with execution rights for this command.

interface vlan

```
interface vlan <VLAN-ID>
no interface vlan <VLAN-ID>
```

Description

Creates an interface VLAN also know as an SVI (switched virtual interface) and changes to the **config-if-vlan** context. The specified VLAN must already be defined on the switch.

The **no** form of this command deletes an interface VLAN.

Parameter	Description
<VLAN-ID>	Specifies the loopback interface ID.
none	Do not reserve any internal VLANs.

Examples

```
switch# config
switch(config)# vlan 10
```

```
switch(config-vlan-10)# exit
switch(config)# interface vlan 10
switch(config-if-vlan)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip address

```
ip address <IP-ADDR>/<MASK> [secondary]
no ip address <IP-ADDR>/<MASK> [secondary]
```

Description

Sets an IPv4 address for the current layer 3 interface.

The **no** form of this command removes the IPv4 address from the interface.

Parameter	Description
<IP-ADDR>	Specifies an IP address in IPv4 format (**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.
`secondary`	Specifies a secondary IP address. (Supported on 6300, except for S3L75A, S3L76A, S3L77A.)

Examples

Setting the IP address on interface **1/1/1** to **192.168.100.1** with a mask of **24** bits:

```
switch(config)# interface 1/1/1
switch(config-if)# ip address 192.168.100.1/24
```

Removing the IP address **192.168.100.1** with a mask of **24** bits from interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# No ip address 192.168.100.1/24
```

Assigning the IP address **192.168.20.1** with a mask of **24** bits to loopback interface **1**:

```
switch(config)# interface loopback 1
switch(config-loopback-if)# ip address 192.168.20.1/24
```

Assigning the IP address **192.168.199.1** with a mask of **24** bits to interface VLAN **10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# ip address 192.168.199.1/24
```

Removing the IP address **192.168.199.1** with a mask of **24** bits from interface VLAN **10**:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no ip address 192.168.199.1/24
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if`
	`config-loopback-if`
	`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. This command is only allowed when routing is enabled on the interface.

Parameter	Description
<VALUE>	Specifies the IP MTU in bytes. Range: 68 to 9198. Default: 1500.

Usage

The IP MTU value for subinterface must be less than or equal to the parent MTU for the subinterface. The subinterface uses its IP MTU value and not the parent IP MTU value.

Examples

Setting the IP MTU to 576 bytes:

```
switch(config-if)# ip mtu 576
```

Setting the IP MTU to the default value:

```
switch(config-if)# no ip mtu
```

Setting the IP MTU value on a subinterface:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip mtu 6000
```

Command History

Release	Modification
10.08	Subinterface support added.
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.

ip source-interface

`ip source-interface {sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-relay | simplivity | dns | all} {interface <IFNAME> | <IPV4-ADDR>} [vrf <VRF-NAME>]`
`no ip source-interface {sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-relay | simplivity | dns | all} [interface <IFNAME> | <IPV4-ADDR>] [vrf <VRF-NAME>]`

Description

Sets a single source IP address for a feature on the switch. This ensures that all traffic sent the feature has the same source IP address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.

This command provides two ways to set the source IP addresses: either by specifying a static IP address, or by using the address assigned to a switch interface. If you define both options, then the static IP address takes precedence.

The `no` form of this command deletes the single source IP address for all supported services, or a specific service.

Parameter	Description
`sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-relay | simplivity | dns | all`	Sets a single source IP address for a specific service. The `all` option sets a global address that applies to all protocols that do not have an address set. For DHCP relay, the address is used as

Parameter	Description
	both the source IP and GIADDR.
`interface <IFNAME>`	Specifies the name of the interface from which the specified service obtains its source IP address. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.
<IPV4-ADDR>	Specifies the source IP address to use for the specified service. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the `default` VRF, if the `vrf` option is not used). Specify the address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.
`vrf <VRF-NAME>`	Specifies the name of a VRF.

Examples

Setting the IPv4 address `10.10.10.5` as the global single source address:

```
switch# config
switch(config)# ip source-interface all 10.10.10.5
```

Setting the secondary IPv4 address `10.10.10.5` on interface `1/1/1` as the global single source address:

```
switch# config
switch(config)# interface 1/1/1
switch(config-if)# ip address 10.10.10.1/24
switch(config-if)# ip address 10.10.10.5/24 secondary
switch(config)# exit
switch(config)# ip source-interface all 10.10.10.5
```

Setting the address `10.10.10.25` on VRF `sflow-vrf` on interface `1/1/2` as the single source address for sFlow:

```
switch(config)# vrf sflow-vrf
switch(config-vrf)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# vrf attach sflow-vrf
switch(config-if)# ip address 10.10.10.25/24
switch(config-if)# exit
switch(config)# ip source-interface sflow interface 1/1/2 vrf sflow-vrf
```

Clearing the global single source IP address **10.10.10.5**:

```
switch(config)# no ip source-interface all 10.10.10.5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip tcp mss

```
ip tcp mss <VALUE>
no ip tcp mss <VALUE>
```

Description

Sets the TCP (Transmission Control Protocol) MSS (Maximum Segment Size) for an interface. When configured, the MSS option in the TCP header is set in the TCP handshake for negotiation during connection establishment. Once the TCP session is established, changing the TCP MSS value on the interface will not affect the existing session.

The **no** form of this command removes the TCP MSS configuration from the interface.

TCP MSS is supported on ROP, SVI, subinterface, and L3 GRE tunnel interface.

Parameter	Description
<VALUE>	Specifies the IPv4 TCP MSS in bytes. Range: 68 to 65495.

Examples

Configuring the IPv4 TCP MSS for the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ip tcp mss 1460
```

Removing the IPv4 TCP MSS configuration from the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ip tcp mss 1460
```

Command History

Release	Modification
10.14.1000	Command introduced.

Command Information

Platforms	Command context	Authority

All platforms	`config-if`
	`config-if-vlan`
	`config-subif`
	`config-gre-if`
		Administrators or local user group members with execution rights for this command.

ip unnumbered

```
ip unnumbered <ifname>
no ip unnumbered <ifname>
```

Description

The IP unnumbered feature allows the switch to process IP packets without configuring a unique IP address on an interface by telling the router to use the IP address of another selected interface as the address for that link. Once set, this port will borrow the user-configured primary IPv4 address from an lender interface and use that IP address in its L3 control plane exchange.

The **no** version of this command removes IP unnumbered support for this port. Once unset, this port will remove borrowed IPv4 address.

Parameter	Description
<Ifname >	Name of the interface

Usage

The port where IP unnumbered is configured is known as the *borrower* interface. Only route-only ports can borrow an address.

The port the address is borrowed from is known as the *lender* interface. Only a loopback interface can be used as a lender interface. The unnumbered interface and lender interface must belong to the same VRF. Additionally, the lender interface for an IP unnumbered interface cannot itself configured as unnumbered.

The following caveats apply to this feature:

- Only the primary IPv4 address can be borrowed on an IP unnumbered interface. You cannot configure a secondary IP address for an interface that is already configured as an IP unnumbered interface.
- If an IP address is configured on an interface that is already configured as an IP unnumbered interface, it will function as a normal IP interface.
- An IPv6 unnumbered configuration on the interface is not supported. If **ip unnumbered** is enabled on the interface, only the IPv4 address is borrowed. However, Any IPv6 configurations can co-exist with an ip unnumbered interface.
- An IP unnumbered interface cannot have multiple lender interfaces for the same address family.
- The **ip unnumbered** command requires that the interface borrowing the address is a routed port. The **IP unnumbered** feature is only supported on devices connected with point-to-point interfaces.
- An unnumbered IP address can not be used as tunnel source.
- The unnumbered interface and lender interface must belong to the same VRF.
- Deleting a lender interface removes all the associated IP unnumbered references.

Examples

Configuring IP unnumbered for a route-only port:

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered loopback1
```

The following examples removes IP unnumbered support for this port. Once unset, this port will remove the borrowed IPv4 address.

```
switch(config)# interface 1/1/1
switch(config-if)# no ip unnumbered loopback1
```

If an IP address is configured on an interface that is already configured as an IP unnumbered interface (or vice versa), both configurations can coexist on the interface. The switch's arbitration logic ensures that static IP configuration is given priority over unnumbered.

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered interface loopback 1
switch(config-if)# ip address 10.16.1.1/24
switch(config-if)# ip address 192.168.1.2/24 secondary

or

switch(config)# interface 1/1/1
switch(config-if)# ip address 10.16.1.1/24
switch(config-if)# ip unnumbered interface loopback 1
switch(config-if)# ip address 192.168.1.2/24 secondary

switch(config)# sh running-config interface
switch(config-if)# do sh running-config interface 1/1/1
interface 1/1/1
   no shutdown
   ip address 10.16.1.1/24
   ip address 192.168.1.2/24 secondary
   ip unnumbered interface loopback 1
     ! ip unnumbered is ignored when static ip is configured
```

If loopback lender interface does not exist during IP unnumbered configuration, a prompt will be displayed in CLI to allow the user to create that interface.

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered interface loopback 1
Lender port not found.
Do you want to create (y/n)? y
switch(config-if)#

Failure case:
switch(config)# ip unnumbered interface loopback 1
Lender port not found.
Do you want to create (y/n)? y
Lender port: loopback1 creation failed
switch(config-if)
```

Command History

Release	Modification
10.14.1000	Command introduced

Command Information

Platforms	Command context	Authority
8320 8325 8325H 8325P 8360 9300 9300S 10000	config-if	Administrators or local user group members with execution rights for this command.

ipv6 address

```
ipv6 address <IPV6-ADDR>/<MASK>{eui64 | [tag <ID>]}
no ipv6 address <IPV6-ADDR>/<MASK>
```

Description

Sets an IPv6 address on the interface.

The **no** form of this command removes the IPv6 address on the interface.

This command automatically creates an IPv6 link-local address on the interface. However, it does not add the **ipv6 address link-local** command to the running configuration. If you remove the IPv6 address, the link-local address is also removed. To maintain the link-local address, you must manually execute the **ipv6 address link-local** command.

Parameter	Description
<IPV6-ADDR>	Specifies the IP address in IPv6 format (**xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**), where **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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 source-interface

```
ipv6 source-interface {sflow |  tftp |  radius | tacacs | ntp | syslog | ubt | dhcp-relay
| simplivity | dns | all} {interface <IFNAME> | <IPV6-ADDR>} [vrf <VRF-NAME>]
no ipv6 source-interface {sflow |  tftp |  radius | tacacs | ntp | syslog | ubt | dhcp-
relay | simplivity | dns | all} [interface <IFNAME> | <IPV6-ADDR>] [vrf <VRF-NAME>]
```

Description

Sets a single source IPv6 address for a feature on the switch. This ensures that all traffic sent the feature has the same source IPv6 address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.

This command provides two ways to set the source IPv6 addresses: either by specifying a static IPv6 address, or by using the address assigned to a switch interface. If you define both options, then the static IPv6 address takes precedence.

The `no` form of this command deletes the single source IPv6 address for all supported protocols, or a specific protocol.

Parameter	Description
`sflow | tftp | radius | tacacs | ntp | syslog | ubt | dhcp-relay | simplivity | dns | all`	Sets a single source IPv6 address for a specific protocol. The `all` option sets a global address that applies to all protocols that do not have an address set.
`interface <IFNAME>`	Specifies the name of the interface from which the specified protocol obtains its source IPv6 address.
<IPV6-ADDR>	Specifies the source IPv6 address to use for the specified protocol. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the `default` VRF, if the `vrf` option is not used). Specify the IP address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.
`vrf <VRF-NAME>`	Specifies the name of the VRF from which the specified protocol sets its source IPv6 address.

Examples

Configuring the IPv6 address `2001:DB8::1` as the global single source address:

```
switch# config
switch(config)# ipv6 source-interface all 2001:DB8::1/32
```

Configuring the IPv6 address `2001:DB8::1` on VRF `sflow-vrf` on interface `1/1/2` as the single source address for sFlow:

```
switch(config)# vrf sflow-vrf
switch(config-vrf)# exit
switch(config)# interface 1/1/2
switch(config-if)# no shutdown
switch(config-if)# vrf attach sflow-vrf
switch(config-if)# ipv6 address 2001:DB8::1/32
switch(config-if)# exit
switch(config)# ipv6 source-interface sflow interface 1/1/2 vrf sflow-vrf
```

Stop the source IPv6 address from using the IP address on interface **1/1/1** on VRF `one`.

```
switch(config)# no ipv6 source-interface all interface 1/1/1 vrf one
```

Clear the source IPv6 address `2001:DB8::1`.

```
switch(config)# no ipv6 source-interface all 2001:DB8::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 tcp mss

```
ipv6 tcp mss <VALUE>
no ipv6 tcp mss <VALUE>
```

Description

Sets the TCP (Transmission Control Protocol) MSS (Maximum Segment Size) for an interface. When configured, the MSS option in the TCP header is set in the TCP handshake for negotiation during connection establishment. Once the TCP session is established, changing the TCP MSS value on the interface will not affect the existing session.

The **no** form of this command removes the TCP MSS configuration from the interface.

TCP MSS is supported on ROP, SVI, subinterface, and L3 GRE tunnel interface.

Parameter	Description
<VALUE>	Specifies the IPv6 TCP MSS in bytes. Range: 68 to 65495.

Examples

Configuring the IPv6 TCP MSS for the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 tcp mss 1440
```

Removing the IPv6 TCP MSS configuration from the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ipv6 tcp mss 1440
```

Command History

Release	Modification
10.14.1000	Command introduced.

Command Information

Platforms	Command context	Authority

All platforms	`config-if`
	`config-if-vlan`
	`config-subif`
	`config-gre-if`
		Administrators or local user group members with execution rights for this command.

l3-counters

```
l3-counters [rx | tx]
no l3-counters [rx | tx]
```

Description

Enables counters on a layer 3 interface. By default, all interfaces are layer 3. To change a layer 2 interface to layer 3, use the **routing** command.

The **no** form of this command, with no specification, disables both transmit and receive counters on a layer 3 interface. To disable transmit (**tx**) or receive (**rx**) counters only, specify the counter type you want to disable.

Parameter	Description
`rx`	Specifies receive counters.
`tx`	Specifies transmit counters.

Examples

Enabling layer 3 transmit counters on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# l3-counters tx
```

Disabling layer 3 transmit and receive counters on interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no l3-counters
```

Layer 3 counters on subinterfaces are only supported on the HPE Aruba Networking 8100and 8360 Switch series.

Enabling layer 3 counters on subinterface **1/1/1.10**:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# l3-counters
```

Disabling layer 3 counters on subinterface **1/1/1.10**:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# no l3-counters
```

Enabling layer 3 receive counters on subinterface **1/1/1.10**:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# l3-counters rx
```

Disabling layer 3 transmit counters on subinterface **1/1/1.10**:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# no l3-counters tx
```

Command History

Release	Modification
10.08	Added support for 13 counters on subinterfaces
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	`config-if` `config-subif`	Administrators or local user group members with execution rights for this command.

mtu

```
mtu <VALUE>
no mtu
```

Description

Sets the MTU (maximum transmission unit) for an interface. This defines the maximum size of a layer 2 (Ethernet) frame. Frames larger than the MTU (1500 bytes by default) are dropped and cause an ICMP fragmentation-needed message to be sent back to the originator.

To support jumbo frames (frames larger than 1522 bytes), increase the MTU as required by your network. A frame size of up to 9198 bytes is supported.

The largest possible layer 1 frame will be 18 bytes larger than the MTU value to allow for link layer headers and trailers.

The **no** form of this command sets the MTU to the default value 1500.

Parameter	Description
<VALUE>	Specifies the MTU in bytes. Range: 46 to 9198. Default: 1500.

Examples

Setting the MTU on interface **1/1/1** to 1000 bytes:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# mtu 1000
```

Setting the MTU on interface **1/1/1** to the default value:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# no mtu
```

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
```

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.
```

Usage

The rate collection interval must be configured in the multiples of 5. Any other value will be rejected and the CLI will display the error message, **The interval must be a multiple of 5.**

Command History

Release	Modification
10.12.1000	Command supported on all platforms.
10.12	Command Introduced on 6300 and 8360 Switch series.

Command Information

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

routing

```
routing
no routing
```

Description

Enables routing support on an interface, creating a L3 (layer 3) interface on which the switch can route IPv4/IPv6 traffic to other devices.

If a user attempts to disable routing for a VNI that has a policy or ACL applied, an appropriate error message is displayed.

By default, routing is enabled on all interfaces.

The **no** form of this command disables routing support on an interface, creating a L2 (layer 2) interface.

If you enable this configuration, collection of flow tracking statistics is disabled.

Examples

Enabling routing support on an interface:

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

Disabling routing support on an interface:

```
switch(config-if)# no routing
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show interface

```
show interface [<IFNNAME>|<IFRANGE>] [brief | physical]
show interface [<IFNNAME>|<IFRANGE>] [extended [non-zero] | [human-readable]]
show interface [<IFNNAME>] monitor [human-readable]
show interface [lag | loopback | tunnel | vlan ] [<ID>] [brief]
show interface lag [<LAG-ID>] [extended [non-zero] | [human-readable]]
show interface lag [<LAG-ID>] monitor [human-readable]
show interface vxlan <VXLAN-ID> [brief | physical]
show interface vxlan <VXLAN-ID> [brief | physical]
```

Description

Shows active configurations and operational status information for interfaces.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
`brief`	Shows brief info in tabular format.
`physical`	Shows the physical connection info in tabular format.
`extended`	Shows additional statistics, including the **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.

Parameter	Description
LOOPBACK	Shows loopback interface information.
TUNNEL	Shows tunnel interface information.
VLAN	Shows VLAN interface information.
<LAG-ID>	Specifies the LAG number. Range: 1-256
<LOOPBACK-ID>	Specifies the LOOPBACK number. Range: 0-255
<TUNNEL-ID>	Specifies the tunnel ID. Range: 1-255
<VLAN-ID>	Specifies the VLAN ID. Range: 1-4094
VXLAN	Shows the VXLAN interface information.
<VXLAN-ID>	Specifies the VXLAN interface identifier. Default: 1

Examples

Showing interface information when it is configured as a route-only port (the **persona** item is only available on the HPE Aruba Networking 10000 Switch Series):

```
switch# show interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Link state: up for 2 days (since Sun Jun 21 05:30:22 UTC 2020)
Link transitions: 1
Description: backup data center link
 Persona: access
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 1500
Type 1GbT
Full-duplex
qos trust none
Speed 1000 Mb/s
Auto-negotiation is on
Flow-control: off
Error-control: off
MDI mode: MDIX
L3 Counters: Rx Enabled, Tx Enabled
Rate collection interval: 300 seconds
Rates                          RX                   TX        Total (RX+TX)
-------------- -------------------- -------------------- --------------------
Mbits / sec                  0.00                 0.00                 0.00
KPkts / sec                  0.00                 0.00                 0.00
Unicast                      0.00                 0.00                 0.00
Multicast                    0.00                 0.00                 0.00
Broadcast                    0.00                 0.00                 0.00
Utilization %                0.00                 0.00                 0.00
Statistics                     RX                   TX                Total
-------------- -------------------- -------------------- --------------------
Packets                         0                    0                    0
Unicast                         0                    0                    0
Multicast                       0                    0                    0
Broadcast                       0                    0                    0
Bytes                           0                    0                    0
```

```
Jumbos                          0                   0                   0
Dropped                         0                   0                   0
Filtered                        0                   0                   0
Pause Frames                    0                   0                   0
L3 Packets                      0                   0                   0
L3 Bytes                        0                   0                   0
Errors                          0                   0                   0
CRC/FCS                         0                 n/a                   0
Collision                     n/a                   0                   0
Runts                           0                 n/a                   0
Giants                          0                 n/a                   0
Other                           0                   0                   0
```

Showing information when the interface is currently linked at a downshifted speed:

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...
Auto-negotiation is on with downshift active
```

Showing information when the interface is shut down during a VSX split (the **persona** item is only available on the HPE Aruba Networking 10000 Switch Series):

```
switch(config-if)# show interface 1/1/1
Interface 1/1/1 is down
Admin state is up
State information: Disabled by VSX
Link state: down for 3 days (since Tue Mar 16 05:20:47 UTC 2021)
Link transitions: 0
Description:
 Persona: access
Hardware: Ethernet, MAC Address: 04:09:73:62:90:e7
MTU 1500
Type SFP+DAC3
Full-duplex
qos trust none
Speed 0 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: 1502-1505
Rate collection interval: 300 seconds

Rate                              RX                  TX        Total (RX+TX)
---------------- -------------------- -------------------- --------------------
Mbits / sec                       0.00                 0.00                 0.00
KPkts / sec                       0.00                 0.00                 0.00
Unicast                           0.00                 0.00                 0.00
Multicast                         0.00                 0.00                 0.00
Broadcast                         0.00                 0.00                 0.00
Utilization                       0.00                 0.00                 0.00

Statistic                         RX                  TX                Total
---------------- -------------------- -------------------- --------------------
Packets                            0                    0                    0
```

```
Unicast                                0                    0                    0
Multicast                              0                    0                    0
Broadcast                              0                    0                    0
Bytes                                  0                    0                    0
Jumbos                                 0                    0                    0
Dropped                                0                    0                    0
Pause Frames                           0                    0                    0
Errors                                 0                    0                    0
CRC/FCS                                0                  n/a                    0
Collision                            n/a                    0                    0
Runts                                  0                  n/a                    0
Giants                                 0                  n/a                    0
```

Showing the monitor information:

In monitor mode, the CLI refreshes data automatically until it is exited by entering **q**. Pressing **?** opens the help menu to display which options are available in this context.

```
Interface 1/1/1 is up
Rate                                RX                   TX        Total (RX+TX)
--------------- -------------------- -------------------- --------------------
MBits / sec                  30196.43             30196.43             60392.85
MPkts / sec                  58977.39             58977.40            117954.79
Unicast                          0.00                 0.00                 0.00
Multicast                    58977.39             58977.40            117954.79
Broadcast                        0.00                 0.00                 0.00
Utilization %                   75.49                75.49               150.98
Statistic                           RX                   TX        Total (RX+TX)
--------------- -------------------- -------------------- --------------------
Packets                    4756527649           4756527865           9513055514
Unicast                             0                    0                    0
Multicast                  4756527649           4756527865           9513055514
Broadcast                           2                    0                    2
Bytes                    304417778668         304417795428         608835574096
Jumbos                              0                    0                    0
Dropped                             0          19028847730          19028847730
Pause Frames                        0                    0                    0
Errors                              0                    0                    0
CRC/FCS                             0                  n/a                    0
help: ?, quit: q
```

```
Help for Interface Monitor
h  Toggle human-readable mode
c  Clear interface statistics
Does not apply to rates
Arrows, PgUp, PgDn, Home, End
Navigate interface statistics
Delay: 2
help: ?, quit: q
```

Showing the output for interface 1/1/1 in human-readable format:

In human-readable format, the **< 1** symbol for **Utilization** indicates that the amount of packets is between zero and one. This is true in cases where the number of bytes increases but the number of packets and the **Utilization** value is not displayed even in the normal output, where the human-readable parameter is not included in the command.

```
switch(config-if)# show interface 1/1/1 human-readable
Interface 1/1/1 is up
Rate                              RX                    TX         Total (RX+TX)
---------------- -------------------- -------------------- --------------------
Bits / sec                        3M                   3M                   6M
Pkts / sec                       316                  316                  633
Unicast                          319                  319                  638
Multicast                          0                    0                    0
Broadcast                          0                    0                    0
Utilization %                  < 1                  < 1                  < 1
Statistic                         RX                   TX                Total
---------------- -------------------- -------------------- --------------------
Packets                         577K                 577K                   1M
Unicast                         577K                 577K                   1M
Multicast                          0                   51                   51
Broadcast                          0                   15                   15
Bytes                           744M                 745M                   1G
Jumbos                             0                    0                    0
Dropped                            0                    0                    0
Filtered                           0                    0                    0
Pause Frames                       0                    0                    0
Errors                             0                    0                    0
CRC/FCS                            0                  n/a                    0
Collision                        n/a                    0                    0
Runts                              0                  n/a                    0
Giants                             0                  n/a                    0
```

Showing information about extended counters:

The output of the `show interface extended` command varies depending on the switch model and configuration.

```
switch(config-if)# show interface 1/1/17 extended
------------------------------------------------------------------------
Interface 1/1/17
------------------------------------------------------------------------
Statistics                                Value
------------------------------------------------------------------------
Dot1d Tp Port In Frames                   547
Dot1d Tp Port Out Frames                  608
Dot3 In Pause Frames                      0
Dot3 Out Pause Frames                     0
Ethernet Stats Broadcast Packets          19
Ethernet Stats Bytes                      40162
Ethernet Stats Packets                    342
...
------------------------------------------------------------------------
Error-Statistics                          Value
------------------------------------------------------------------------
Dot1d Base Port MTU Exceeded Discards     0
Dot3 Control In Unknown Opcodes           0
Dot3 Stats Alignment Errors               0
Dot3 Stats FCS Errors                     0
Dot3 Stats Frame Too Longs                0
Dot3 Stats Internal Mac Transmit Errors   0
Ethernet RX Oversize Packets              0
...
```

Showing interface link-status:

```
switch# show interface link-status
------------------------------------------------------------


Port           Type           Physical    Link         Last
                              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           --
```

Showing state information when interface is blocked:

```
8360(config-if)# show interface 1/1/1

Interface 1/1/1 is up (Blocked)
Admin state is up
State information: Blocked by UDLD
```

```
Link state: up for 1 minute (since Mon Jun 10 09:25:27 UTC 2024)
Link transitions: 1
Description:
Persona:
Hardware: Ethernet, MAC Address: 00:fd:45:67:85:91
MTU 1500
Type 10G-LR / 10G SFP+ LR
Full-duplex
qos trust none
Speed 10000 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: access
Access VLAN: 1
Rate collection interval: 300 seconds

Rate                              RX                  TX        Total (RX+TX)
---------------- -------------------- -------------------- --------------------
Mbits / sec                     0.00                 0.00                 0.00
KPkts / sec                     0.00                 0.00                 0.00
Unicast                         0.00                 0.00                 0.00
Multicast                       0.00                 0.00                 0.00
Broadcast                       0.00                 0.00                 0.00
Utilization %                   0.00                 0.00                 0.00
Statistic                         RX                   TX                Total
---------------- -------------------- -------------------- --------------------
Packets                           15                   15                   30
Unicast                           12                   12                   24
Multicast                          3                    3                    6
Broadcast                          0                    0                    0
Bytes                           1350                 1350                 2700
Jumbos                             0                    0                    0
Dropped                            0                    0                    0
Pause Frames                       0                    0                    0
Errors                             0                    0                    0
CRC/FCS                            0                  n/a                    0
Collision                        n/a                    0                    0
Runts                              0                  n/a                    0
Giants                             0                  n/a                    0
```

Command History

Release	Modification
10.15	Added state information when port goes into down state.
10.11	Added `monitor` parameter.
10.10	Added `human-readable` parameter.
10.09	Added persona information for the 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 interface dom

```
show interface [<INTERFACE-ID>] dom [detail] [vsx-peer]
```

Description

Shows diagnostics information and alarm/warning flags for the optical transceivers (SFP, SFP+, QSFP+). This information is known as DOM (Digital Optical Monitoring). DOM information also consists of vendor determined thresholds which trigger high/low alarms and warning flags.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**.
`detail`	Show detailed information.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

```
switch# show interface dom
--------------------------------------------------------------------------------
Port    Type      Channel  Temperature 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show interface flow-control

```
show interface [<IFNNAME>|<IFRANGE>] flow-control [detail]
```

Description

Shows the flow control configuration, status, and statistics of the specified interface for interfaces on which flow control is enabled.

If **detail** is not specified, this command shows a summary of all flow controlled interfaces with one interface per line. If **detail** is specified, this command shows flow control detailed statistics.

As of AOS-CX 10.10, the separate **show flow-control** command has been removed, with it being effectively replaced by this command.

Parameter	Description
<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
```

Command History

Release	Modification
10.10	Examples updated with new and changed output elements.
10.08	Command introduced.

Command Information

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

show interface link-diagnostics

`show interface [<IFNNAME>|<IFRANGE>] link-diagnostics`

Description

Shows information about select link diagnostics, including MAC, PHY, and Transceiver diagnostics.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
link-diagnostics	Shows link diagnostics information.

Examples

Showing interface information for 1/1/12 link diagnostics:

```
switch# show interface 1/1/12 link-diagnostics
------------------------------------------------------------------------------
Interface 1/1/12           Current State             Changes         Last Change
------------------------------------------------------------------------------
Port Status                Waiting for link
Link Down Reason           Local fault

Transceiver
No transceiver             --                              0         --
TX Fault                   --                              0         --
Transceiver error          --                              0         --
System error               --                              0         --
DOM error                  --                              0         --
Configuring transceiver    --                              0         --
Transceiver disabled       --                              0         --
Transceiver unsupported    --                              0         --
MAC and PHY
TX Disabled                --                              0         --
Autoneg Incomplete         --                              0         --
No Signal Detected         --                              0         --
No RX Lock                 True                            1         22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Remote Fault               --                              0         --
Local Fault                True                            1         22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Link State                 Down                            1         16 seconds ago
(Tue Nov 14 14:30:54 UTC 2023)
switch# show interface 1/1/12 link-diagnostics
------------------------------------------------------------------------------
Interface 1/1/12           Current State             Changes         Last Change
------------------------------------------------------------------------------
Port Status                Link up
Link Down Reason           --

Transceiver
No transceiver             --                               0         --
TX Fault                   --                               0         --
Transceiver error          --                               0         --
System error               --                               0         --
DOM error                  --                               0         --
Configuring transceiver    --                               0         --
Transceiver disabled       --                               0         --
Transceiver unsupported    --                               0         --
MAC and PHY
TX Disabled                --                               2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Autoneg Incomplete         --                               0         --
No Signal Detected         --                               2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
No RX Lock                 --                               2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Remote Fault               --                               2         21 seconds
ago (Tue Nov 14 14:30:49 UTC 2023)
Local Fault                --                               2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
  Link State               Up                               1         16 seconds
ago (Tue Nov 14 14:30:54 UTC 2023)
```

Showing interface information for 1/1/7-1/1/8 link-diagnostics:

```
switch# show interface 1/1/7-1/1/8 link-diagnostics
------------------------------------------------------------------------------
Interface 1/1/7            Current State             Changes         Last Change
 ----------------------------------------------------------------------------
Port Status                Link up
Link Down Reason           --

Transceiver
No transceiver             --                          0         --
TX Fault                   --                          0         --
Transceiver error          --                          0         --
 System error              --                          0         --
DOM error                  --                          0         --
Configuring transceiver    --                          0         --
Transceiver disabled       --                          0         --
Transceiver unsupported    --                          0         --
MAC and PHY
TX Disabled                --                          2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Autoneg Incomplete         --                          0         --
No Signal Detected         --                          2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
 No RX Lock                --                          2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Remote Fault               --                          2         21 seconds
ago (Tue Nov 14 14:30:49 UTC 2023)
 Local Fault               --                          2         22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
 Link State                Up                          1         16 seconds
ago (Tue Nov 14 14:30:54 UTC 2023)
------------------------------------------------------------------------------
Interface 1/1/8            Current State             Changes         Last Change
------------------------------------------------------------------------------
Port Status                Link up
Link Down Reason           --

Transceiver
No transceiver             --                          0         --
 TX Fault                  --                          0         --
Transceiver error          --                          0         --
System error               --                          0         --
 DOM error                 --                          0         --
 Configuring transceiver   --                          0         --
Transceiver disabled      --                          0         --
Transceiver unsupported   --                          0         --
 MAC and PHY
TX Disabled               --                          2         22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Autoneg Incomplete         --                          0         --
No Signal Detected         --                          2         22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
No RX Lock                 --                          2         22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
 Remote Fault              --                          2         21 seconds ago
(Tue Nov 14 14:30:49 UTC 2023)
Local Fault                --                          2         22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Link State                 Up                          1         16 seconds ago
(Tue Nov 14 14:30:54 UTC 2023)
```

Command History

Release	Modification
10.14	Command introduced.

Command Information

Platforms	Command context	Authority
8325 9300 9300P	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface profile

```
show interface [<IFNAME> | <IFRANGE>] profile
```

Description

Displays the profile information for each interface.

Parameter	Description
<IFNAME>	Specifies the interface name.
<IFRANGE>	Specifies the interface range.

Examples

Displaying the profile information for each interface:

```
switch# show interface profile
-------------------------------------------------
          Profile             Profile
Port      Type        Active  Membership
-------------------------------------------------
...
1/1/17    --          yes     --
1/1/17:1  split       yes     profile-1 profile-2
1/1/17:2  split       yes     profile-1 profile-2
1/1/17:3  split       yes     profile-1 profile-2
1/1/17:4  split       yes     profile-1 profile-2
1/1/18    --          yes     --
1/1/18:1  split       yes     profile-1
1/1/18:2  split       yes     profile-1
1/1/18:3  split       yes     profile-1
1/1/18:4  split       yes     profile-1
```

Command History

Release	Modification
10.15	Command supported on the 9300 Switch Series
10.14	Command introduced on the 9300S Switch Series.

Command Information

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

show interface statistics

```
show interface [<IFNAME>|<IFRANGE>] statistics [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] statistics monitor [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] error-statistics [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] error-statistics monitor [non-zero] [human-readable]
show interface lag [<LAG-ID>] statistics [non-zero] [human-readable]
show interface lag [<LAG-ID>] statistics monitor [non-zero] [human-readable]
show interface lag [<LAG-ID>] error-statistics [non-zero] [human-readable]
show interface lag [<LAG-ID>] error-statistics monitor [non-zero] [human-readable]
show interface vxlan <VXLAN-ID> statistics [non-zero] [human-readable]
```

Description

Shows statistics for switch interfaces such as packets transmitted and received, bytes transmitted and received, broadcast and multicast packets.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
LAG	Shows LAG interface information.
<LAG-ID>	Specifies the LAG number. Range: 1-256
VXLAN	Shows the VXLAN interface information.
<VXLAN-ID>	Specifies the VXLAN interface identifier. Default: 1
monitor	Continuously monitor interface statistics.
human-readable	Shows statistics rounded to the nearest power of 1000, for example, 1K, 345M, 2G.
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    Runts    CRC/FCS   Collisions
-------------------------------------------------------------------------------------
1/1/1                          190          20   100647        0          0            0
1/1/10                           0           0      100      290       7165          949
1/1/11                           0           0        0        0          0            0
1/1/12                           0           0        0        0          0            0
...
1/1/30 - lag1                 1500         500    45800        0          0            0
1/1/31 - lag2                    0           0       11       27          0            0
1/1/32 - lag2                    0           0        0        0          6           18
```

Showing monitor statistics:

The rows and columns of show interface monitor statistics depends on the length of width of the client terminal. The CLI can be navigated using the arrow keys as well as the PageUp, PageDown, Home, and End keys.

```
show interface statistics monitor
-------------------------------------------------------------------
Interface                          RX Bytes          RX Packets >>
-------------------------------------------------------------------
1/1/1                         3440525421984          53758209526
1/1/2                         3440526607008          53758228042
1/1/3                         3440527785312          53758246453
1/1/30                        3440559671264          53758744653
1/1/31                        3440560851680          53758763098
1/1/32                        3440562028704          53758781489

                                                    help: ?, quit: q
```

```
Help for Interface Monitor

f    Toggle full statistics
h    Toggle human-readable mode
n    Toggle non-zero mode
r    Toggle rate display

c    Clear interface statistics
       Does not apply to rates

Arrows, PgUp, PgDn, Home, End
       Navigate interface statistics

Delay:2
                                                                help: ?, qui
```

Showing monitor error statistics in human-readable format:

```
show interface 1/1/1-1/1/3,1/1/30-1/1/32 error-statistics monitor human-readable
-------------------------------------------------------------------------------------------------
Interface               RX Errors    TX Errors    RX Giants    RX Runts      CRC/FCS  Collisions
-------------------------------------------------------------------------------------------------
1/1/1                           0            0            0           0            0           0
1/1/2                           0            0            0           0            0           0
1/1/3                           0            0            0           0            0           0
1/1/30                          0            0            0           0            0           0
1/1/31                          0            0            0           0            0           0
1/1/32                          0            0            0           0            0           0


Human-readable                                                      help: ?, quit: q
```

```
Help for Interface Monitor

h    Toggle human-readable mode
n    Toggle non-zero mode

c    Clear interface statistics
       Does not apply to rates

Arrows, PgUp, PgDn, Home, End
       Navigate interface statistics

Delay:2
                                                          help: ?, quit: q
```

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] [vsx-peer]`

Description

Displays information about transceivers present in the switch. The information shown varies for different transceiver types and manufacturers. Only basic information is shown for unsupported HPE and third-party transceivers installed in the switch and they are also identified with an asterisk in the output.

Parameter	Description
<INTERFACE-ID>	Specifies the name or range of an interface on the switch. Use the format **member/slot/port** (for example, **1/3/1**).
`detail`	Show detailed information for the interfaces.
`threshold-violations`	Show threshold violations for transceivers.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing summary transceiver information with identification of unsupported transceivers:

```
switch(config)# show interface transceiver
---------------------------------------------------------------------
Port      Type           Product      Serial          Part
Number       Number          Number
---------------------------------------------------------------------
1/1/1     SFP+SR         J9150A       MYxxxxxxxx      1990-3657
1/1/2     SFP+ER*        --           --              --
1/2/1     QSFP+SR4       JH233A       MYxxxxxxxx      2005-1234
1/2/2     QSFP+ER4*      --           --              --
1/3/1     SFP28DAC3      844477-B21   MYxxxxxxxx      77fc-7ce7
```

```
* unsupported transceiver
```

Showing detailed transceiver information:

```
switch(conf#) show interface transceiver detailing
Transceiver in 1/1/1
   Interface Name     : 1/1/1
   Type               : SFP+SR
   Connector Type     : LC
   Wavelength         : 850nm
   Transfer Distance  : 0m (SMF), 30m (OM1), 80m (OM2), 300m (OM3)
   Diagnostic Support : DOM
   Product Number     : J9150A
   Serial Number      : MYxxxxxxx
   Part Number        : 1990-3657

Status
   Temperature : 47.65C
   Voltage     : 3.31V
   Tx Bias     : 8.40mA
   Rx Power    : 0.08mW, -10.96dBm
   Tx Power    : 0.56mW, -2.49dBm

Recent Alarms :
   Rx power low alarm
   Rx power low warning
   Recent Errors :
   Rx loss of signal

Transceiver in 1/1/2
   Interface Name     : 1/1/2
   Type               : unknown
   Connector Type     : ??
   Wavelength         : ??
   Transfer Distance  : ??
   Diagnostic Support : ??
   Product Number     : ??
   Serial Number      : ??
   Part Number        : ??

Transceiver in 1/2/1
   Interface Name     : 1/2/1
   Type               : QSFP+SR4
   Connector Type     : MPO
   Wavelength         : 850nm
   Transfer Distance  : 0m (SMF), 0m (OM1), 0m (OM2), 100m (OM3)
   Diagnostic Support : DOM
   Product Number     : JH233A
   Serial Number      : MYxxxxxxx
   Part Number        : 2005-1234

Status
   Temperature : 44.46C
   Voltage     : 3.30V

---------------------------------------------
          Tx Bias  Rx Power     Tx Power
Channel#  (mA)     (mW/dBm)     (mW/dBm)
---------------------------------------------
1         6.12     0.00, -inf   0.63, -1.95
```

```
2          6.04     0.00, -inf   0.63, -2.00
3          6.51     0.00, -inf   0.60, -2.16
4          6.19     0.00, -inf   0.63, -1.94

Recent Alarms :
 Channel 1 :
   Rx power low alarm
   Rx power low warning
 Channel 2 :
   Rx power low alarm
   Rx power low warning
 Channel 3 :
   Rx power low alarm
   Rx power low warning
 Channel 4 :
   Rx power low alarm
   Rx power low warning

Recent Errors :
 Channel 1 :
   Rx Loss of Signal
 Channel 2 :
   Rx Loss of Signal
 Channel 3 :
   Rx Loss of Signal
 Channel 4 :
   Rx Loss of Signal

Transceiver in 1/2/2
  Interface Name     : 1/2/2
  Type               : unknown
  Connector Type     : ??
  Wavelength         : ??
  Transfer Distance  : ??
  Diagnostic Support : ??
  Product Number     : ??
  Serial Number      : ??
  Part Number        : ??

Transceiver in 1/3/1
  Interface Name     : 1/3/1
  Type               : SFP28DAC3
  Connector Type     : Copper Pigtail
  Transfer Distance  : 0.00km (SMF), 0m (OM1), 0m (OM2), 0m (OM3)
  Diagnostic Support : None
  Product Number     : 844477-B21
  Serial Number      : MYxxxxxxx
  Part Number        : 77fc-7ce7
```

Showing detailed transceiver information with identification of unsupported transceivers:

```
Transceiver in 1/1/2
 Interface Name      : 1/1/2
 Type                : SFP+ER (unsupported)
 Connector Type      : LC
 Wavelength          : 3590nm
 Transfer Distance   : 80m (SMF), 0m (OM1), 0m (OM2), 0m (OM3)
 Diagnostic Support  : DOM
 Vendor Name         : INNOLIGHT
 Vendor Part Number  : TR-PX15Z-NHP
 Vendor Part Revision: 1A
```

```
 Vendor Serial number: MYxxxxxxx

Status
 Temperature : 28.88C
 Voltage     : 3.30V
 Tx Bias     : 65.53mA
 Rx Power    : 0.00mW, -inf
 Tx Power    : 1.47mW, 1.67dBm

Recent Alarms:
 Rx Power low alarm
 Rx Power low warning
 Recent Errors:
```

Showing transceiver threshold-violations:

```
switch(config)# show interface transceiver threshold-violations
-----------------------------------------------------
Port      Type         Channel  Type(s) of Recent
                                Threshold Violation(s)
-----------------------------------------------------
1/1/1     SFP+SR                Tx bias high warning
                                50.52 mA > 40.00 mA
1/1/2     SFP+ER*               ??
1/2/1     QSFP+SR4    1         Tx power low alarm
                                -17.00 dBm < -0.50 dBm
                      2         Tx bias low warning
                                3.12 mA < 4.00 mA
1/2/2     QSFP+ER4*             ??
1/3/1     SFP28DAC3             n/a
* unsupported transceiver
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show interface supported-transceivers

`show interface {<IFNAME>|<IFRANGE>} supported-transceivers`

Description

Displays transceivers supported by a specific, or all, interface(s) in the switch. Information varies and is dependent on transceiver types, part number, and short description or interfaces.

Parameter	Description
IFNAME	Specifies the name of an interface on the switch. Use the following format: member/slot/port. Example: 1/3/1
IFRANGE	Specifies the name of an interface range on the switch. Use the following format: member/slot/port. Example: 1/1/1-1/1/2

Example

Showing a full switch interface or chassis switch with multiple line modules:

```
switch# show interface supported-transceivers
--------------------------------------------------------------------------
Type               Product          Supported
                   Number           Interfaces
--------------------------------------------------------------------------
1G-BT              JL747            1/1/33-1/1/34
1G-BT              J8177            1/1/33-1/1/34
1G-LH              J4860            1/1/33-1/1/34
IG-LX              J4859            1/1/33-1/1/34
8x25G-DAC2         S4B39            1/1/2,1/1/4,1/1/6,1/1/8,1/1/10,1/1/12,1/1/14,
                                    1/1/16,1/1/18,1/1/20,1/1/22,1/1/24,1/1/26,
                                    1/1/28,1/1/30,1/1/32
QSA28              845970           1/1/1-1/1/32

Note: For full product numbers (SKUs) with revision letters,
refer to the transceiver guide.
```

```
switch# show interface supported-transceivers
--------------------------------------------------------------------------
Type               Product          Supported
                   Number           Interfaces
--------------------------------------------------------------------------
100M-FX            J9054            1/10/1-1/10/24,1/12/1-1/12/48
1G-BT              JL747            1/5/49-1/5/52,1/7/25-1/7/28,1/8/25-1/8/28,
                                    1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48
10G-BT             JL563            1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,
                                    1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,
                                    1/12/1-1/12/48
10G-BiDi-D         R9X54            1/4/1-1/4/12,1/6/1-1/6/36,1/11/1-1/11/12,
                                    1/12/1-1/12/48
10G-SR             J9150            1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,
                                    1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,
                                    1/10/1-1/10/28,1/11/1-1/11/12,1/12/1-1/12/48
10G-SR             JL782            1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12
25G-AOC15          R0Z21            1/6/1-1/6/32
25G-AOC7           R0M45            1/6/1-1/6/32
25G-BiDi-10-U      S1C98            1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,
8x50G-DAC2         S4B42            1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,
                                    1/8/25-1/8/28,1/9/49-1/9/52,1/10/25-1/10/28,
                                    1/12/1-1/12/48
QSA28              845970           1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12

Note: For full product numbers (SKUs) with revision letters,
refer to the transceiver guide.
```

Showing a single interface:

```
switch# show interface 1/1/1 supported-transceivers
------------------------------------------------------------------------
Type               Product          Description
                   Number
------------------------------------------------------------------------
Interface 1/1/1

10G-BiDi-D @       R9X54            10G BX-D 40km
10G-BiDi-U @       R9X55            10G BX-U 40km
100G-LR4           JL310            100G QSFP28 LR4
100G-SR1.2         S4B44            100G SR1.2 Q28 LC
100G-SR2           S1C93            100G MPO SR2
100G-SR4           JL309            100G QSFP28 SR4
QSA28              845970           --

@ This transceiver is only supported when inserted in a QSA

For full product numbers (SKUs) with revision letters, refer to the Transceiver
guide.
```

Showing a range of interfaces:

```
switch# show interface 1/1/1-1/1/2 supported-transceivers
------------------------------------------------------------------------
Type               Product          Description
                   Number
------------------------------------------------------------------------
Interface 1/1/1

10G-BiDi-D @       R9X54            10G BX-D 40km
10G-BiDi-U @       R9X55            10G BX-U 40km
10G-ER @           S2P32            10G SFP+ ER
100G-SR2           S1C93            100G MPO SR2
100G-SR4           JL309            100G QSFP28 SR4
QSA28              845970           --
Interface 1/1/2

10G-BiDi-D @       R9X54            10G BX-D 40km
10G-BiDi-U @       R9X55            10G BX-U 40km
10G-ER @           S2P32            10G SFP+ ER
25G-BiDi-10-D @    S1C96            25G LC BiDi 10km-D
25G-SR @           S2P33            25G SFP28 SR
40G-eSR4           JH233            QSFP+ eSR4
100G-BiDi          845972           --
100G-SR4           JL309            100G QSFP28 SR4
QSA28              845970           --

@ This transceiver is only supported when inserted in a QSA

For full product numbers (SKUs) with revision letters, refer to the Transceiver
guide.
```

Showing a chassis switch with muliple line modules:

```
switch# show interface supported-transceivers
------------------------------------------------------------------------
Type            Product     Supported
                      Number      Interfaces
------------------------------------------------------------------------
```

```
100M-FX          J9054       1/10/1-1/10/24,1/12/1-1/12/48
1G-BT            JL747       1/5/49-1/5/52,1/7/25-1/7/28,1/8/25-1/8/28,
                             1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48
10G-BT           JL563       1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,
                             1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,
                             1/12/1-1/12/48
10G-BiDi-D       R9X54       1/4/1-1/4/12,1/6/1-1/6/36,1/11/1-1/11/12,
                             1/12/1-1/12/48
10G-SR           J9150       1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,
                             1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,
                             1/10/1-1/10/28,1/11/1-1/11/12,1/12/1-1/12/48
10G-SR           JL782       1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12
25G-AOC15        R0Z21       1/6/1-1/6/32
25G-AOC7         R0M45       1/6/1-1/6/32
25G-BiDi-10-U    S1C98       1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,
8x50G-DAC2       S4B42       1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,
                             1/8/25-1/8/28,1/9/49-1/9/52,1/10/25-1/10/28,
                             1/12/1-1/12/48
QSA28            845970      1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12

For full product numbers (SKUs) with revision letters, refer to the Transceiver
guide.
```

Showing a VSF stack:

```
switch# show interface supported-transceivers
 ------------------------------------------------------------------------------
Type             Product          Supported
                 Number           Interfaces
 ------------------------------------------------------------------------------
100M-FX          J9054            1/1/1-1/1/24,2/1/1-2/1/48
1G-BT            JL747            1/1/49-1/1/52,3/1/25-3/1/28,4/1/25-4/1/28
10G-BT           JL563            1/1/49-1/1/52,2/1/1-2/1/32,3/1/25-3/1/28,
                                  4/1/25-4/1/28
10G-AOC15        721076           1/1/13,1/1/15-1/1/27,1/1/41-1/1/42
10G-AOC5         Q9S66            1/1/13,1/1/15-1/1/27,1/1/41-1/1/42
25G-AOC15        R0Z21            3/1/1-3/1/32
QSA28            845970           4/1/1-4/1/12,2/1/33-2/1/36,1/1/1-1/1/12

For full product numbers (SKUs) with revision letters, refer to the Transceiver
guide.
```

Showing an empty chassis:

```
switch# show interface supported-transceivers
No available interfaces.
```

Command History

Release	Modification
10.16.1000	Command introduced

Command Information

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

show interface utilization

```
show interface [<IFNNAME>|<IFRANGE>] utilization [non-zero]
```

Description

Displays physical port throughput and utilization.

Parameter	Description
<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   --
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip interface

```
show ip interface <INTERFACE-ID>|{lag|loopback|vlan|tunnel <ID>}
```

Description

Shows status and configuration information for an IPv4 interface. Note the following caveats for the HPE Aruba Networking 10000 Series switches:

- When this command is issued for a subinterface, the output of the command displays only the aggregate packet count of L3 packets passing through the switch.
- When this command is issued for a subinterface, the output of this command does not display L3 counters .
- If the selected subinterface is shut, the L2 counter will be reset to 0. When the subinterface is reenabled, the L2 counter will be reset to 0.

Parameter	Description
<INTERFACE-ID>	Specifies the name of an interface. Format: **member/slot/port**.
`lag <ID>`	Show LAG interface information, where <ID> is 1-256.
`loopback <ID>`	Show loopback interface information, where <ID> is 0-255.
`tunnel <ID>`	Show tunnel interface information, where <ID> is 1-255.
`vlan <ID>`	Show VLAN interface information, where <ID> is 1-4094.

Example

```
switch# show ip interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IP MTU 1500
IP TCP MSS 1460
IPv4 address 192.168.1.1/24
L3 Counters: Rx Enabled, Tx Enabled
Statistic                          RX                   TX                  Total
---------------- -------------------- -------------------- --------------------
L3 Packets                          0                    0                      0
L3 Bytes                            0                    0                      0
```

```
switch# show ip interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
IP MTU 1500
```

```
IP TCP MSS 1460
IP Directed Broadcast is Disabled
IPv4 address 2.2.2.2/32 [unnumbered to loopback1]
L3 Counters: Rx Disabled, Tx Disabled
```

```
switch# show ip interface loopback 1
Interface loopback1 is up
Admin state is up
Hardware: Loopback
IP Directed Broadcast is Disabled
IPv4 address 192.168.1.1/24
```

Command History

Release	Modification
10.14.1000	Command output can display information for an IP unnumbered interface and IP TCP MSS configuration.
10.07 or earlier	--

Command Information

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

show ip source-interface

```
show ip source-interface {sflow |  tftp |  radius | tacacs | all} [vrf <VRF-NAME>]
     [vsx-peer]
```

Description

Shows single source IP address configuration settings.

Parameter	Description
`sflow | tftp | radius | tacacs | all`	Shows single source IP address configuration settings for a specific protocol. The **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.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
Showing single source IP address configuration settings for sFlow:
switch# show ip source-interface sflow
Source-interface Configuration Information
----------------------------------------
Protocol        Source Interface
--------        ----------------
sflow            10.10.10.1
```

Showing single source IP address configuration settings for all protocols:

```
switch# show ip source-interface all
Source-interface Configuration Information
----------------------------------------
Protocol        Source Interface
--------        ----------------
all             1/1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ipv6 interface

`show ipv6 interface <INTERFACE-ID> [vsx-peer]`

Description

Shows status and configuration information for an IPv6 interface. Note the following caveats for the HPE Aruba Networking 8325, 10000 Series switches:

- When this command is issued for a subinterface, the output of the command displays only the aggregate packet count of L3 packets passing through the switch.
- When this command is issued for a subinterface, the output of this command does not display L3 counters .
- If the selected subinterface is shut, the L2 counter will be reset to 0. When the subinterface is reenabled, the L2 counter will be reset to 0.

Parameter	Description
<INTERFACE-ID>	Specifies an interface ID. Format: **member/slot/port**.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

```
switch# show ipv6 interface 1/1/1
Interface 1/1/1 is up
  Admin state is up
  IPv6 address:
    2001:0db8:85a3:0000:0000:8a2e:0370:7334/24 [VALID]
  IPv6 link-local address: fe80::1e98:ecff:fee3:e800/64 (default)[VALID]
  IPv6 virtual address configured: none
  IPv6 multicast routing: disable
  IPv6 Forwarding feature: enabled
  IPv6 multicast groups locally joined:
    ff02::ff70:7334  ff02::ffe3:e800  ff02::1  ff02::1:ff00:0
    ff02::2
  IPv6 multicast (S,G) entries joined: none
  IPv6 MTU: 1524 (using link MTU)
  IPv6 TCP MSS 1440
  IPv6 unicast reverse path forwarding: none
  IPv6 load sharing: none
  RX
          0 packets, 0 bytes
  TX
          0 packets, 0 bytes
```

```
switch# show ipv6 interface 1/1/14.1
Interface 1/1/14.1 is up
  Admin state is up
    IPv6 address:
      30::1/64 [VALID]
    IPv6 link-local address: fe80::b86a:97c0:122:2f42/64 [VALID]
    IPv6 virtual address configured: none
    IPv6 multicast routing: disable
    IPv6 Forwarding feature: enabled
    IPv6 multicast groups locally joined:
      ff02::1  ff02::1:ff22:2f42  ff02::1:ff00:1  ff02::1:ff00:0
      ff02::2
    IPv6 multicast (S,G) entries joined: none
    IPv6 MTU 1500
    IPv6 TCP MSS 1440
    IPv6 unicast reverse path forwarding: none
    IPv6 load sharing: none
Encapsulation dot1q ID: 20
```

```
switch# show ipv6 interface lag2.1
Interface lag2.1 is up
  Admin state is up
    IPv6 address:
      40::1/64 [VALID]
    IPv6 link-local address: fe80::b86a:97c0:122:2f42/64 [VALID]
    IPv6 virtual address configured: none
    IPv6 multicast routing: disable
    IPv6 Forwarding feature: enabled
    IPv6 multicast groups locally joined:
      ff02::1  ff02::1:ff22:2f42  ff02::1:ff00:1  ff02::1:ff00:0
      ff02::2
    IPv6 multicast (S,G) entries joined: none
    IPv6 MTU 1500
    IPv6 TCP MSS 1440
    IPv6 unicast reverse path forwarding: none
```

```
    IPv6 load sharing: none
  Encapsulation dot1q ID: 30
```

Command History

Release	Modification
10.14.1000	Command output can display information for an IP unnumbered interface and IPv6 TCP MSS configuration.
10.07 or earlier	--

Command Information

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

show ipv6 source-interface

```
show ipv6 source-interface {sflow |  tftp |  radius | tacacs | all} [vrf <VRF-NAME>]
     [vsx-peer]
```

Description

Shows single source IP address configuration settings.

Parameter	Description
`sflow | tftp | radius | tacacs | all`	Shows single source IP address configuration settings for a specific protocol. The **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.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing single source IP address configuration settings for sFlow:

```
switch# show 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        Source Interface
--------        ----------------
 all             1/1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show system interface-group

```
show system interface-group
        detail
        line-module <slot-id>
               map

        member <member-id>
```

Description

Displays the configuration and status of interface groups.

Parameter	Description
detail	Show detailed interface group information
line-module <slot-id>	Show information for a line module slot ID (for example, **1/1**).
map	For 8325 Switch series, show a map of ports and speed groups.
member <member-id>	Show information for a single VSF member

Examples

The output in the following commands vary, depending on switch model.

Show basic interface group status

```
switch# show system interface-group
```

```
-----------------------------------------------
Group  Speed  Member Ports      Mismatched Ports
-----------------------------------------------
1      10g    1/1/1-1/1/12
2      25g    1/1/13-1/1/24     1/1/13
3      25g    1/1/25-1/1/36
4      25g    1/1/37-1/1/48
```

Show detailed interface group status, including allowed speeds of each.

```
switch# show system interface-group detail
-------------------------------------------------------------------------
Allowed                Mismatched
Module  Group  Ports       Option    Speeds                  Ports
-------------------------------------------------------------------------
1/6     1      1-8          25g @+*  10g,25g
50g      50g
1/6     2      9-16         25g   *  10g,25g
50g @+   50g                    9-16
1/6     3      17-24        25g @+*  10g,25g
50g      50g
1/6     4      25-32        25g   *  10g,25g
50g @+   50g
@ Currently applied setting
+ Configured setting
* Default setting
```

Show a map of ports and speed groups on a 8325 Switch series;

```
switch# show system interface-group map
Port
1    4    7   10   13   16   19   22   25   28   31   34   37   40   43   46
================================================================================
|  5 |  6 |  6 |  7 |  8 |  9 |  9 | 10 | 11 | 12 | 12 | 13 | 14 | 15 | 15 | 16 |
--------------------------------------------------------------------------------
|  5 |  6 |  7 |  7 |  8 |  9 | 10 | 10 | 11 | 12 | 13 | 13 | 14 | 15 | 16 | 16 |
--------------------------------------------------------------------------------
|  5 |  5 |  6 |  7 |  8 |  8 |  9 | 10 | 11 | 11 | 12 | 13 | 14 | 14 | 15 | 16 |
================================================================================
```

Command History

Release	Modification
10.16.1010	The **map** parameter introduced on 8325 Swith series.
10.12	Command introduced

Command Information

Platforms	Command context	Authority
8325 8360 9300S 10040	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show system interface-profile

```
show system interface-profile
```

Description

Displays the configuration and status of interface profiles.

Examples

Displaying the configuration and status of the system interface profile.

```
switch# show system interface-profile
-------------------------------------------------------
        Profile     Default     Configured  Active
Module  Type        Profile     Profile     Profile
-------------------------------------------------------
1/1     split       profile-1   profile-1   profile-1
```

Command History

Release	Modification
10.15	Command supported on the 9300 Switch Series
10.14	Command introduced.

Command Information

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

shutdown

```
shutdown
no shutdown
```

Description

Disables an interface. Interfaces are disabled by default when created.

The **no** form of this command enables an interface.

Examples

Disabling an interface:

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

Enabling an interface:

```
switch(config-if)# no shutdown
```

Command History

Release	Modification
10.07 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> [override] | <SPEED-DUPLEX> | auto [<SPEED>] [override]}
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

Parameter	Description
	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.
`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.
`override`	Override the detected transceiver speed and use the configured speed.

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 <SPEED> override`

Uses a fixed speed with no auto-negotiation. If the currently installed transceiver does not support the speed, attempt to use it anyway. This may or may not work, depending on the transceiver.

`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.

`speed auto <SPEED> override`

Uses auto-negotiation and offers only the specified speed. If the currently installed transceiver does not support auto-negotiation, attempt to use it anyway. This may or may not work depending on the transceiver.

- Override support is not available on optical transceivers.
- Speed override and auto-negotiation override are not supported on split ports.
- Auto-negotiation cannot be enabled on a 10G-DAC .

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
```

Command History

Release	Modification
10.11	**speed <*SPEED*> override** and **speed auto <*SPEED*> override** are added. This is available only on HPE Aruba Networking 8100, 8360, 8325, and 10000 Switch Series.
10.09.0001	Speeds not supported by hardware hidden by CLI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 10000	`config-if`	Administrators or local user group members with execution rights for this command.

split

```
split [<COUNT>][<SPEED>][confirm]
no split [confirm]
```

Description

Splits a port into multiple interfaces. Only ports capable of supporting breakout cables or SR4/eSR4/eDR4 optics can be split.

Parameter	Description
<COUNT>	Specifies the number of child interfaces to activate upon splitting the port. Default: 4.
<SPEED>	Specifies the speed for the child interfaces.
`confirm`	Specifies the confirmation of port splitting.

Usage

- Some switch interfaces support different split counts depending on the installed transceiver. For these interfaces, the number of child interfaces to activate can be specified. If omitted, the default is 4. For transceivers capable of supporting multiple split modes, the closest mode with enough lanes is used.
- Some transceivers also support multiple split modes with different speeds. For example, 2x200G or 2x100G. When a speed is not specified, the highest available speed for the split count is used. To select a different split mode with a lower speed, the desired speed must be specified.

When the current transceiver does not support the configured split speed, the interface will remain down with an `Invalid speed` error.

Ports that are not splittable in the currently applied interface profile can be configured as split, but remain in a **down** state until a compatible profile is selected and the switch rebooted to apply it.

The splittable ports for all models are shown in the table below:

Model	Description	Port info
8320 Series ■ JL479A	8320 48 10/6 40 X472 5 2 Bundle	49-54 (40G)

Model	Description	Port info
■ JL579A ■ JL581A	8320 32 40G X472 5 2 Bundle 8320 48 T/6 40 X472 5 2 Bundle	5-28 (40G - center 24 ports) 49-54 (40G)
8325 Series		
■ JL635A ■ JL624A ■ JL625A ■ JL626A ■ JL627A ■ JL636A	8325-48Y8C 48p 25G 8p 100G switch 8325-48Y8C FB 6 F 2 PS Bundle 8325-48Y8C BF 6 F 2 PS Bundle JL626A 8325-32C FB 6 F 2 PS Bundle 8325-32C BF 6 F 2 PS Bundle 8325-32C 32p 100G switch	49-56 (40G or 100G) 49-56 (40G or 100G) 49-56 (40G or 100G) 1-32 (40G or 100G) 1-32 (40G or 100G) 1-32 (40G or 100G)
8360 32Y4C models JL717A (base system) ■ JL700A Port-to-Power model ■ JL701A Power-to-Port model	8360-32Y4C switch 8360-32Y4C switch	33-36 (40G or 100G) 33-36 (40G or 100G)
8360 16Y2C models JL718A (base system) ■ JL702A Port-to-Power model ■ JL703A Power-to-Port model	8360-16Y2C switch 8360-16Y2C switch	17-18 (40G or 100G) 17-18 (40G or 100G)
8360 48XT4C models JL720A (base system) ■ JL706A Port-to-Power model ■ JL707A Power-to-Port model	8360-48XT4C switch 8360-48XT4C switch	NO SUPPORT for Split ports
8360-12C models JL721A (base system) ■ JL708A Port-to-Power model ■ JL709A Power-to-Port model	8360-12C switch 8360-12C switch	1-12 (40G or 100G) 1-12 (40G or 100G)
8360 24XF2C models JL722A (base system) ■ JL710A Port-to-Power model ■ JL711A Power-to-Port model	8360-24XF2C switch 8360-24XF2C switch	25-26 (40G or 100G) 25-26 (40G or 100G)
9300 Switch Series ■ R8Z96A	9300-32D 32p 100/200/400G QSFP-DD p 10G SFP+ Switch	Porte 1-32 are splittable. 400G SR8 can split two, four, or eight ways (8-way splitting available on the 9300-32D only). Some ports are splittable depending on the interface profile use. See the Installation and Getting Started Guide for more information.
9300S Switch Series		

Model	Description	Port info
▪ S0F95A ▪ S0F96A	9300S 32P QSFP28 100G 8p QSFP-DD 400G TAA Switch 9300S 32P QSFP28 100G 8p QSFP-DD 400G Switch	9-12. 17-24, and 29-32 ports are splittable. 400G SR8 can split two or four ways QSFP-DD ports are capable of operating at: ▪ 100G ports ▪ 40G ports ▪ Split into 4 individual 25G or 10G ports Some ports are splittable depending on the interface profile use. See the Installation and Getting Started Guide for more information.
10000 Switch Series ▪ R8P13A	10000-48Y6C FB6F2PS Bundle	Ports 49-54 are splittable. QSFP28 ports are capable of operating as: ▪ 100G ports ▪ 40G ports ▪ Split into 4 individual 25G or 10G ports
▪ R8P14A	10000-48Y6C BF6F2PS Bundle	Ports 49-54 are splittable. QSFP28 ports are capable of operating as: ▪ 100G ports ▪ 40G ports ▪ Split into 4 individual 25G or 10G ports

Examples

Before splitting an interface (example on a 8325 Series Switch):

```
switch(config)# show interface 1/1/56 brief
--------------------------------------------------------------------------------
Port    Native  Mode   Type      Enabled Status Reason                Speed Desc
        VLAN
--------------------------------------------------------------------------------
1/1/56  --      routed QSFP+DA1  no      down   Administratively down --    --
```

After splitting:

```
switch(config)# interface 1/1/56
switch(config-if)# split
This command will disable the specified port, clear its configuration,
and split it into multiple interfaces.
```

```
Continue (y/n)? y

8325(config-if)# show interface 1/1/56,1/1/56:1-1/1/56:4 brief
--------------------------------------------------------------------------------
Port      Native Mode   Type       Enabled Status  Reason           Speed   Desc
          VLAN                                                      (Mb/s)
--------------------------------------------------------------------------------
1/1/56    --     routed QSFP+DA1   no      down    Interface split  --      --
1/1/56:1  --     routed QSFP+DA1   yes     up                       10000   --
1/1/56:2  --     routed QSFP+DA1   yes     up                       10000   --
1/1/56:3  --     routed QSFP+DA1   yes     up                       10000   --
1/1/56:4  --     routed QSFP+DA1   yes     up                       10000   --
```

Unsplitting a port on a switch that does not require a reboot:

```
switch(config)# interface 1/1/1
switch(config-if)# no split
This command will disable the split interfaces for this port and clear
their configuration.

Continue (y/n)? y
```

Splitting an interface two ways on a 9300 Series Switch using the default for speed, taking the port capability (400G), and assuming 200G:

```
switch(config)# interface 1/1/1
switch(config-if)# split 2
This command will disable the specified port, clear its configuration,
and split it into multiple interfaces.

Continue (y/n)? y

switch(config-if)# show interface brief
--------------------------------------------------------------------------------
Port     Native  Mode   Type       Enabled Status  Reason    Speed   Description
         VLAN                                               (Mb/s)
--------------------------------------------------------------------------------
1/1/1:1   --     routed 400G-SR8    yes     up              200000
1/1/1:2   --     routed 400G-SR8    yes     up              200000
```

Changing the interface to 2x100G mode:

```
switch(config)# interface 1/1/1
switch(config-if)# split 2 100g
This command will clear the configuration for all split interfaces of
this port.

Continue (y/n)? y

switch(config-if)# show interface brief
--------------------------------------------------------------------------------
Port     Native  Mode   Type       Enabled Status  Reason    Speed   Description
         VLAN                                               (Mb/s)
--------------------------------------------------------------------------------
1/1/1:1   --     routed 400G-SR8    yes     up              100000
1/1/1:2   --     routed 400G-SR8    yes     up              100000
```

Command History

Release	Modification
10.10.1000	Added parameters: ***<COUNT>*** , **<SPEED>**
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	`config-if`	Administrators or local user group members with execution rights for this command.

system interface-group

This command is not available on the HPE Aruba Networking 8100 Switch Series.

```
system interface-group <GROUP> speed <SPEED>
no system interface-group <GROUP> speed <SPEED>
```

Description

Configures the speed for an interface group. After changing group speed, only transceivers compatible with the new speed will be enabled.

- All speed-mismatched interfaces in the group will be disabled.
- This command can interrupt active network links, user confirmation is required to proceed.

The **no** form of this command resets the specified interface group to its default.

Parameter	Description
<GROUP>	Specifies the interface group to configure.
<SPEED>	Configures transceiver speed (10g, 25g or 50g) for a group. Default is 25g (see the *Transceiver Guide* for further detail). Configures transceiver speed (10g or 25g) for a group. Default is 25g (see the *Transceiver Guide* for further detail). On HPE Aruba Networking 8325 Switch Series: **10g** allows 1Gbps or 10Gbps transceivers only. **25g** allows 25Gbps transceivers only.

Parameter	Description
	On HPE Aruba Networking 9300/9300S Switch Series: **10g** allows 1Gbps or 10Gbps transceivers only. **25g** allows 25Gbps transceivers only. For HPE Aruba Networking 8360 Switch Series: For the latest information on supported speeds for each model of 8360 Switch, refer to the **Network Ports** section of the 8360 Hardware Installation Guide. On HPE Aruba Networking 10000 Switch Series: 10g allows 1Gbps or 10Gbps transceivers only. 25g allows 25Gbps transceivers only.

Examples

Configuring interface group 1 to allow 10Gbps and slower transceivers:

```
switch(config)# system interface-group 1 speed 10g
Changing the group speed will disable all member interfaces that do not match the
new speed.

Continue (y/n)? y
```

Command History

Release	Modification
10.10.1000	Command introduced on 9300 and 10000 Switch series.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 9300 9300S 10000	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

system interface-profile

```
system interface-profile {split} <NAME>
no system interface-profile {split} <NAME>
```

Description

Configures the status of split interface profiles.

The **no** form of this command removes the specified interface profile.

Parameter	Description
`{split}`	Configures a splittable interface profile.
<NAME>	Specifies the one of the following two profile names: ■ profile-1 ■ profile-2

Usage

Some switch models have hardware resource allocation options for different applications. For example, a switch that cannot support splitting all ports for use with breakout cables may have a profile to maximize 100G links and another profile to maximize 25G links.

Switch Model	Profile Name	Splittable Ports	Split Modes Available
930032D	profile-1 (default)	1-32	2 x 100/200G, 4 x 10/25/50/100G
	profile-2	2-32 even	2 x 100/200G, 4 x 10/25/50/100G, 8 x 10/25/50G* **NOTE:** Only QSFP-DD ports can split eight ways
9300S	profile-1 (default)	9-12 17-24 29-32	2 x 100G 2 x 100/200G, 4 x10/25/50/100G 2 x 100G
	profile-2	13, 15, 16 17, 19, 21, 23 25, 26, 27	4 x 10/25G 2 x 100/200G, 4 x 10/25/50/100G 4 x 10/25G

Splittable ports from any profile can always be configured as split interfaces, but the children can only establish a link when the switch is booted with a profile where that port is splittable. For example, port 1/1/16 can be split at any time, but only establishes a link on the child interfaces when the switch is booted with **profile-2** configured. Child ports that are not members of the booted profile remain down with a reason of **Split profile mismatch**.

After changing the configured profile, the switch must be rebooted before that profile is applied. Configuring a new profile does not change the configured split setting for any interfaces. It also does not affect any split interfaces that are not members of the new profile until the switch is rebooted.

Examples

Configuring the switch to use 4x100g breakout cables in ports 17-20:

```
switch(config)# system interface-profile split profile-1
switch(config)# interface 1/1/17-1/1/20
switch(config-if-<1/1/17-1/1/20>)# split 4 100g
```

Configuring the switch to use 4x25g breakout cables in port 16:

```
switch(config)# system interface-profile split profile-2
This command requires a reboot to apply. After reboot, any ports not compatible
with the new profile will be disabled.
Continue (y/n)? y

switch(config)# interface 1/1/16
switch(config-if-<1/1/16>)# split 4 25g
```

Configuring the switch to use 2x100g breakout cables in port 9-12:

```
switch(config)# system interface-profile split profile-1
This command requires a reboot to apply. After reboot, any ports not compatible
with the new profile will be disabled.
Continue (y/n)? y

switch(config)# interface 1/1/9-1/1/12
switch(config-if-<1/1/9-1/1/12>)# split 2 100g
```

Command History

Release	Modification
10.14	Command introduced.

Command Information

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

DSM commands

clear dsm statistics

`clear dsm <SLOT-ID> statistics [global]`

Description

Clears the statistics of the interfaces attached to the distributed services module.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.
`global`	Clears the DSM interface statistics for all sessions.

Examples

Clearing the DSM interface statistics:

```
switch(config)# clear dsm statistics
switch(config)# clear dsm 1/1 statistics
switch(config)# clear dsm 1/2 statistics global

Warning: clearing statistics globally will be reflected in all CLI
sessions, any agents running in the analytics engine, and any external
systems monitoring switch statistics.
Continue (y/n)? y
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

diag dsm console

`diag dsm console <SLOT-ID>`

Description

Provides access to the operator console of the attached distributed services module. From this console, operator commands can be run. Exiting the console returns the user back to CLI. This is intended for diagnostic purposes only.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.

Examples

Accessing the DSM console **1/1**:

```
switch(config)# diagnostic
switch(config)# diag dsm console 1/1
Distributed Services module 1/1 is ready
IP 169.254.13.1
# pwd
/root
# exit
Connection to 169.254.13.1 closed.
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

dsm

```
dsm
no dsm
```

Description

Creates the DSM configuration context in the switch.

Examples

Creating a DSM:

```
switch(config)# dsm
switch(config-dsm)#
  erspan              Enable ERSPAN for DSM
  ip-all              IPv4 and IPv6 information
  ipfix               Enable IPFIX for DSM
  show                Show running system information
  uplink-to-uplink    Enable network to network traffic on L3VNI and L2VNI
  workload-migration  Enable migration of workloads across Distributed Service
                      Switches
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

erspan

```
erspan
no erspan
```

Description

Enables the Encapsulated Remote Switched Port Analyzer (ERSPAN) functionality in DSM.

The **no** form of this command disables the ERSPAN functionality in DSM.

Examples

Enabling ERSPAN for DSM:

```
switch(config-dsm)# erspan
ERSPAN is enabled for DSM
```

Disabling ERSPAN for DSM:

```
switch(config-dsm)# no erspan
ERSPAN is disabled for DSM
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config-dsm`	Administrators or local user group members with execution rights for this command.

ipfix

```
ipfix
no ipfix
```

Description

Enables the IPFIX functionality in DSM.

The **no** form of this command disables the IPFIX functionality in DSM.

Examples

Enabling IPFIX:

```
switch(config-dsm)# ipfix
```

Disabling IPFIX:

```
switch(config-dsm)# no ipfix
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config-dsm`	Administrators or local user group members with execution rights for this command.

dsm uplink-to-uplink

```
dsm uplink-to-uplink
no dsm uplink-to-uplink
```

Description

For ports that are associated with an uplink type persona using the **persona uplink** command, use this command to bypass policy-enforcement for L3 and L3-VxLAN flows between these ports. thereby allowing the forwarding of traffic between them.

The **no** form of this command disables this feature.

Examples

Enabling the DSM uplink-to-uplink feature.

```
switch(config)# dsm
switch(config-dsm)# uplink-to-uplink
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config-dsm`	Administrators or local user group members with execution rights for this command.

workload-migration

```
workload-migration
no workload-migration
```

Description

Enables the workload migration across Distributed Service Switches.

The **no** form of this command disables the workload migration across Distributed Service Switches.

Examples

Enabling workload migration:

```
switch(config-dsm)# workload-migration
```

Disabling workload migration:

```
switch(config-dsm)# no workload-migration
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	config-dsm	Administrators or local user group members with execution rights for this command.

show dsm

show dsm *<SLOT-ID>*

Description

Displays the the information about the distributed services module

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.

Examples

Showing the DSM information:

```
switch(config)# show dsm
Distributed Services Modules
============================
Product Serial
Name Number Description Number Status
---- --------------- ------------------------------------ ------------
1/1 DSS-4825-6100 Distributed Services Module FSJ21280004 ready
1/2 DSS-4825-6100 Distributed Services Module FSJ21280004 ready
```

Showing the DSM **1/2** information:

```
switch(config)# show dsm 1/2
Distributed services module 1/2 is ready
Description : Distributed Services Module
Full Description :
Serial number : FSJ21280004
Product number : DSS-4825-6100
MAC Address : 04:90:81:00:1d:d4
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm erspan

`show dsm erspan`

Description

Displays the status of the Encapsulated Remote Switched Port Analyzer (ERSPAN) feature for DSM.

Examples

Showing the workload migration status:

```
switch(config)# show dsm erspan
ERSPAN is enabled
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm ipfix

`show dsm ipfix`

Description

Displays the status of IPFIX for DSM.

Examples

Showing the IPFIX status:

```
switch(config)# show dsm ipfix
IPFIX is enabled
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm uplink-to-uplink

```
show dsm uplink-to-uplink
```

Description

Show whether the DSM uplink-to-uplink feature is enabled or disabled.

Examples

Showing the status of the DSM uplink-to-uplink feature

```
switch(config)# show dsm uplink-to-uplink
Uplink to uplink is enabled
```

Command History

Release	Modification
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm interface statistics

```
show dsm <SLOT-ID> interface statistics {non-zero}
```

Description

Displays the information about the interfaces attached to the distributed services module.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.
`non-zero`	Shows interfaces with at least one non-zero statistics. Optional.

Examples

Showing the DSM interface statistics:

```
switch(config)# show dsm 1/1 interface statistics
-------------------------------------------------------------------------
Interface   RX Bytes   RX Packets  RX Drops  TX Bytes  TX Packets  TX Drops
-------------------------------------------------------------------------
1           0          0           0         0         0           0
2           518        7           0         0         0           0
3           0          0           0         0         0           0
4           188        2           0         0         0           0
Total       706        9           0         0         0           0

-------------------------------------------------------------------------------
Interface RX Broadcast RX Multicast TX Broadcast TX Multicast RX Pause TX Pause
-------------------------------------------------------------------------------
1         0            0            0            0            0        0
2         0            7            0            0            0        0
3         0            0            0            0            0        0
4         0            2            0            0            0        0
Total     0            9            0            0            0        0
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm redirect vlan

`show dsm <SLOT-ID> redirect vlan <VLAN-ID>`

Description

Displays the information about the VLANs redirected to the distributed services module and which address family each VLAN is in. If applicable, it will show a list of VLANs that could not be applied.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.
<VLAN-ID>	Shows the specified VLANs. Range 1 to 4094.

Examples

Showing all VLANs redirected to DSM **1/1**:

```
switch(config)# show dsm 1/1 redirect
Distributed Services Modules 1/1
====================================
VLANs: 2-4,1024
        Address Family: IPv4  (4/4 applied)
VLANs: 1024
        Address Family: IPv6  (1/1 applied)
```

Showing VLANs in range **1000-1010** redirected to DSM **1/1**:

```
switch(config)# show dsm 1/1 redirect vlan 1000-1010
Distributed Services Modules 1/1
====================================
VLANs: 1008-1010
       Address Family: IPv4  (3/3 applied)
No IPv6 VLAN redirect configured to this Distributed Services module
```

Showing all redirected VLANs:

```
switch(config)# show dsm redirect
Distributed Services Modules 1/2
====================================
VLANs: 1013,1016
Configured but unapplied: 1014-1015
        Address Family: IPv4  (2/4 applied)
VLANs: 1013,1016
Configured but unapplied: 1014-1015
        Address Family: IPv6  (2/4 applied)

Distributed Services Modules 1/1
====================================
VLANs: 1001-1002
Configured but unapplied: 1003
        Address Family: IPv4  (2/3 applied)
VLANs: 1001-1002
Configured but unapplied: 1003
        Address Family: IPv6  (2/3 applied)
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm statistics

`show dsm <SLOT-ID> statistics`

Description

Displays the statistics of the distributed services module.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.

Examples

Showing the DSM interface statistics:

```
switch(config)# show dsm 1/1 statistics
Statistic                          RX                  TX                  Total
 ---------------- -------------------- -------------------- --------------------
 Packets                            10                    0                   10
   Unicast                           0                    0                    0
   Multicast                        10                    0                   10
   Broadcast                         0                    0                    0
 Bytes                             780                    0                  780
 Jumbos                              0                    0                    0
 Dropped                             0                    0                    0
 Filtered                           10                    0                   10
 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
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	config	Administrators or local user group members with execution rights for this command.

show dsm vrf

`show dsm <SLOT-ID> vrf <VRF-NAME>`

Description

Displays the information about the VRFs redirected to the distributed services module.

Parameter	Description
<SLOT-ID>	Shows the slot ID of the DSM.

Parameter	Description
<VRF-NAME>	Shows the specified VRF.

Examples

Showing the redirected VRFs:

```
switch(config)# show dsm vrf
Distributed Services Modules 1/2
====================================
VRFs: VRF10, VRF11
        Address Family: IPv4
No IPv6 VRF redirect configured to this Distributed Services module

Distributed Services Modules 1/1
====================================
VRFs: VRF12, VRF14
        Address Family: IPv4
No IPv6 VRF redirect configured to this Distributed Services module
```

Showing the redirected VRFs for a DSM 1/1:

```
switch(config)# show dsm 1/1 vrf
Distributed Services Modules 1/1
====================================
VRFs: VRF12, VRF14
        Address Family: IPv4
No IPv6 VRF redirect configured to this Distributed Services module
```

Showing the redirected VRFs for a DSM 1/1:

```
switch(config)# show dsm 1/1 vrf VRF12
Distributed Services Modules 1/1
====================================
VRFs: VRF12
        Address Family: IPv4
No IPv6 VRF redirect configured to this Distributed Services module
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

show dsm workload-migration

```
show dsm workload-migration
```

Description

Displays the status of workload migration across Distributed Service Switches.

Examples

Showing the workload migration status:

```
switch(config)# show dsm workload-migration
Workload migration is enabled
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
10000	`config`	Administrators or local user group members with execution rights for this command.

Chapter 6
Subinterfaces

A subinterface is a virtual interface created by dividing one physical interface into multiple logical interfaces. Subinterfaces use the parent physical interface for sending and receiving data.

Subinterfaces are not supported on 8320 switch series.

Supported features

The following features are supported on L3 subinterfaces:

- RoP, L3 LAG and Hydra interface (split cable) support
- IPv4/IPv6 addressing
- ARP/ND
- Static unicast routing (IPv4/IPv6)
- Unicast routing (IPv4/IPv6) - OSPF and VRRP
- Unicast routing (IPv4/IPv6) - BGP and IVRL
- IPv4/IPv6 multicast routing (IGMP and PIM)
- Ingress ACLs and Ingress Policies
- MTU (maximum transmission unit)
- L3 counters
- VSX keep alive links
- SNMP read
- REST support

For the 8325 and 10000 Switch series, IVRL subinterfaces are not supported.

IPv4/IPv6 multicast routing, ingress ACLs and Ingress Policies, and VSX keep alive links are not supported on the 9300 switch series.

Configuring subinterfaces

- Subinterfaces can be configured for physical ports, split children of physical ports and L3 LAG interfaces.
- Subinterfaces on multiple ports can be assigned the same VLAN ID (there is no bridging between subinterfaces or between subinterfaces and SVIs) using `encapsulation vlan-idencapsulation vlan-id`. Each subinterface is considered to be in a separate bridge domain.
- The IP-MTU of a subinterface can be configured independent of the parent port's IP-MTU configuration.

Procedure

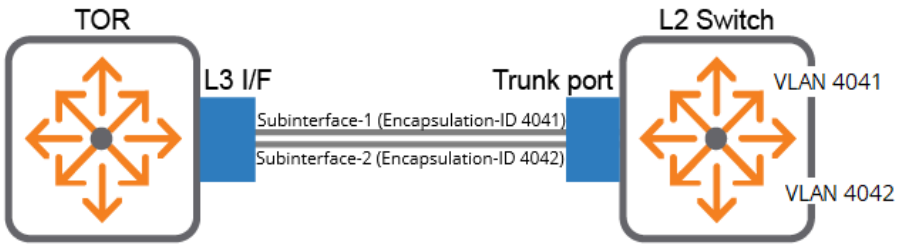
One router with one physical interface needs to be connected to two IP networks:

1. Create two subinterfaces within the physical interface.
2. Assign each subinterface an IP address within each subnet.
3. Route packets between the two subnets.

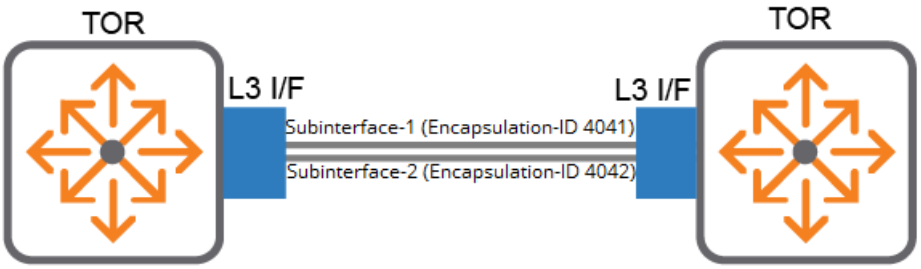
Limitations

- Subinterfaces can only be configured on L3 ports with routing enabled.
- A subinterface cannot be a member of a LAG.
- An L3 parent interface with subinterfaces cannot be a member of a LAG.
- An L3 parent interface with subinterfaces cannot be used for L3 services (for example IP address configuration is not supported on an L3 interface if the interface is configured with subinterfaces).
- On physical interfaces, each subinterface must have a unique encapsulation ID.

Subinterface in a router-on-a-stick deployment



- Top-of-rack switch/router with an L3 interface connected to the trunk port of an L2 switch.
- Routing tables configured to forward outgoing traffic through a subinterface while applying a VLAN ID tag.
- All outgoing traffic from the L3 interface is tagged with a VLAN ID which enables the switch to forward traffic through different VLANs.



- Top-of-rack switch/router with an L3 interface connected to the trunk port of an L3 interface.
- Routing tables configured to forward outgoing traffic through a subinterface while applying a VLAN ID tag.
- All outgoing traffic from the L3 interface is tagged with a VLAN ID which enables the switch to forward traffic through different VLANs.

Subinterface commands

Configuration of **system internal-vlan-range** to **2000-3200** is required on the HPE Aruba Networking 8325 and 10000 Switch series for scaled subinterfaces. Refer to the *L2 Bridging Guide* for more information on **system internal-vlan-range**.

encapsulation dot1q

```
encapsulation dot1q <VLAN-ID>
no encapsulation dot1q <VLAN-ID>
```

Description

Configures 802.1Q encapsulation on a subinterface.

The **no** form of this command removes 802.1Q encapsulation on a subinterface.

Parameter	Description
<VLAN-ID>	Specifies encapsulation VLAN ID. Range 1 to 4094. **NOTE:** The encapsulation VLAN ID should be unique within an L3 LAG subinterface. The same encapsulation VLAN ID can be configured among different parent interfaces, but the encapsulation VLAN ID should not be configured in the internal VLAN range. (Encapsulation VLAN IDs and static VLANs are entirely different and do not coincide.)

Usage

Associates an 802.1Q VLAN ID with a subinterface.

Examples

Configuring 802.1Q encapsulation on a subinterface:

```
switch(config)# interface 1/1/1.201
switch(config-subif)# encapsulation dot1q 10
```

Removing 802.1Q encapsulation on a subinterface:

```
switch(config-subif)# no encapsulation dot1q 10
```

Command History

Release	Modification
10.16	Command introduced for 9300 Switch series.
10.11	Command introduced for 8325, 10000 Switch series.
10.08	Command introduced for the, and 8360 switch series.

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 9300 8360 10000	config-subif	Administrators or local user group members with execution rights for this command.

interface

```
interface <IFNAME>.<ID>
no interface <IFNAME>.<ID>

interface lag <LAGNUM>.<ID>
no interface lag <LAGNUM>.<ID>
```

Description

Creates a subinterface on an L3 interface and enters subinterface configuration mode. The subinterface name consists of the parent interface name (for example, 1/1/1) followed by a period and a unique ID number.

The **no** form of these commands deletes a subinterface from an L3 interface.

8325, 8325H, 8325P, and 10000 Switch series require an internal VLAN for every subinterface, in addition to the internal VLANs used for other purposes. For example, to support 1024 subinterfaces, an internal VLAN range that is at least that large must be reserved using the **system internal-vlan-range** command. 8325, 8325H, 8325P, and 10000 Series switches support a maximum of 1024 subinterfaces resources.

BFD sessions are not supported on sub interfaces on 9300 Switch series. Use switch virtual interfaces (SVIs) to configure a BFD session on these switch models.

Parameter		Description
	<IFNAME>	Specifies L3 interface name.
	<ID>	Specifies subinterface ID. Range 1 to 4094.
	<LAGNUM>	Specifies L3 LAG interface number.

Usage

To create a LAG subinterface, the parent LAG must exist before creating the subinterface.

Each LAG subinterface requires four internal VLANs . You can configure a combination of L3 LAG subinterfaces and physical interface subinterfaces. Each L3 LAG consumes four sub-interface resources, and in this LAG there can be maximum of four LAG member interfaces. Each physical interface sub-interface consumes one sub-interface resource.

Examples

Creating a subinterface on L3 interface 1/1/1.201 and entering subinterface configuration mode:

```
switch(config)# interface 1/1/1.201
switch(config-subif)#
```

Deleting subinterface on L3 interface 1/1/1.201:

```
switch(config)# no interface 1/1/1.201
```

Creating a subinterface on an L3 LAG port and entering subinterface configuration mode:

```
switch(config)# interface lag 1
switch(config-if)# interface lag 1.201
switch(config-subif)#
```

Deleting subinterface on an L3 LAG port :

```
switch(config)# no interface lag 1.201
```

Command History

Release	Modification
10.16	Command introduced for 9300 Switch series.
10.11	Command introduced for 8325 and 10000 Switch series.
10.08	Command introduced for the, and 8360 switch series.

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 9300 10000	`config`	Administrators or local user group members with execution rights for this command.

show capacities subinterface

```
show capacities subinterface
```

Description

Displays maximum subinterface capacity.

Examples

Showing maximum subinterface capacity:

```
switch# show capacities subinterface

System Capacities: Filter Subinterface
Capacities Name
Value
-------------------------------------------------------------------------------
-
Maximum number of LAG subinterfaces for the entire system
256
Maximum number of LAG members when the LAG has subinterfaces
4
Maximum number of normal subinterfaces for the entire system
1024
Maximum number of subinterface resources for the entire system (normal+(4*LAG)
1024
```

Command History

Release	Modification
10.16	Command introduced for 9300 Switch series.
10.11	Command introduced for 8325 and 10000 Switch series.
10.08	Command introduced for the , and 8360 switch series.

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 9300 10000	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show interface

```
show interface <IFNAME>.<ID>
show interface lag <LAGNUM>.<ID>
```

Description

Displays a subinterface configuration.

Parameter		Description
	<IFNAME>	Specifies L3 interface name.
	<ID>	Specifies subinterface ID.
	<LAGNUM>	Specifies L3 LAG interface number.

Examples

Showing subinterface configuration:

```
switch# show interface 1/1/1.201
Interface 1/1/1.201 is down
Admin state is up
State information: Waiting for link
Description:
Hardware: Ethernet, MAC Address: 38:21:c7:5a:80:80
Encapsulation dot1Q ID: 10
Statistic                          RX                  TX                  Total
---------------- -------------------- -------------------- --------------------
L3 Packets                          0                   0                   0
L3 Bytes                            0                   0                   0
```

Showing subinterface LAG configuration:

```
switch# show interface lag1.1
Interface lag1.1 is down
Admin state is up
Description:
Hardware: Ethernet, MAC Address: 38:21:c7:5a:80:80
Encapsulation dot1Q ID: 2
Statistic                          RX                  TX                  Total
---------------- -------------------- -------------------- --------------------
L3 Packets                          0                   0                   0
L3 Bytes                            0                   0                   0
```

Command History

Release	Modification
10.16	Command introduced for 9300 Switch series.
10.11	Command introduced for 8325 and 10000 Switch series.
10.08	Command introduced for the 8360 switch series.

Command Information

Platforms	Command context	Authority
8100 8325 8325H 8325P 8360 9300 10000	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

Chapter 7
Source interface selection

The source IP address is determined by the system and is typically the IP address of the outgoing interface in the routing table. However, routing switches may have multiple routing interfaces and outgoing packets can potentially be sent by different paths at different times. This results in different source IP addresses.

AOS-CX provides a configuration model that allows the selection of an IP address to use as the source address for all outgoing traffic. This allows unique identification of the software application on the server site regardless of which local interface has been used to reach the destination server. The source interface selection supports selecting an IP address or interface name.

If the source interface and source IP are configured, Source IP will have priority.

Source-interface selection commands

ip source-interface

```
ip source-interface <PROTOCOL> {<IP-ADDR>|interface <IFNAME>} [vrf <VRF-NAME>]
no ip source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]
```

Description

Configures the IPv4 source-interface interface to use for the specified protocol. If a VRF is not given, the default VRF applies.

The **no** form of this command removes the specified configuration.

Parameter	Description
<PROTOCOL>	Specifies the protocol to configure. ■ **all**: Selects the source for all protocols covered by this command. ■ **central**: Selects HPE Aruba Networking Central. ■ **dhcp_relay**: Selects DHCP relay. When you configure a dhcp_ relay source interface, you must also enable DHCP relay Option 82 using the **dhcp-relay option 82 source-interface** command. ■ **dns**: Selects DNS. ■ **erspan**: Selects ERSPAN. Only supported on the 10000 Switch Series. ■ **http**: Selects HTTP. ■ **ipfix**: Selects ipfix. Configures source interface for IPFIX. ■ **ntp**: Selects NTP. ■ **psm**: Selects PSM. Only supported on the 10000 Switch Series. ■ **ptp**: Selects PTP.

Parameter	Description
	■ **radius**: Selects RADIUS. ■ **sflow**: Selects sFLow. ■ **sftp-scp**: Selects SFTP and SCP. ■ **ssh-client**: Selects SSH Client. ■ **syslog**: Selects the source for syslog packets. ■ **tacacs**: Selects the source for TACACS packets. ■ **tftp**: Selects TFTP. ■ **workload_migratio**n: Selects workload migration. Only supported on the 10000 Switch Series.
<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
```

Command History

Release	Modification
10.12.1000	Added **central, sftp-scp**, and **ssh-client** parameters.
10.07 or earlier	--

Command Information

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

ipv6 source-interface dns

```
ipv6 source-interface {dns  |all} {interface | X:X::X:X} [vrf <VRF-NAME>]
[no] ipv6 source-interface {dns | all} {interface | X:X::X:X} [vrf <VRF-NAME>]
```

Description

Configures the IPv6 source-interface or source IP for IPv6 DNS clients.

The **no** form of this command removes all configurations.

Parameter	Description
<IPV6-ADDR>	Specifies the IPv6 address.
`vrf <VRF-NAME>`	Specifies the VRF name.

Examples

Configuring IPv6 source-interface DNS on 1: :1:

```
switch(config)# ipv6 source-interface dns 1::1
vrf   VRF Configuration
```

Configuring IPv6 source-interface DNS on 1: :1 vrf **red**

```
switch(config)# ipv6 source-interface dns 1::1 vrf red
switch(config)# ipv6 source-interface dns interface vlan10
vrf   VRF Configuration
```

Configuring IPv6 source-interface DNS on VLAN 10 and vrf **red**:

```
switch(config)# ipv6 source-interface dns interface vlan10 vrf red
```

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.

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. ■ **all**: Selects the source for all protocols covered by this command. ■ **central**: Selects HPE Aruba Networking Central. ■ **dhcp_relay**: Selects DHCP relay. When you configure a dhcp_ relay source interface, you must also enable DHCP relay Option 82 using the **dhcp-relay option 82source-interface** command. ■ **dns**: Selects DNS. ■ **http**: Selects HTTP. ■ **ipfix**: Selects ipfix. Configures source interface for IPFIX. ■ **ntp**: Selects NTP. ■ **ptp**: Selects PTP. ■ **radius**: Selects RADIUS. ■ **sflow**: Selects sFLow. ■ **sftp-scp**: Selects SFTP and SCP. ■ **ssh-client**: Selects SSH Client. ■ **syslog**: Selects the source for syslog packets. ■ **tacacs**: Selects the source for TACACS packets. ■ **tftp**: Selects TFTP.
<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
```

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.

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 HPE Aruba Networking Central.

Parameter	Description

	`dhcp relay`
	Shows the source interface configuration for DHCP relay.
	`dns`
	Shows the source interface configuration for DNS.
	`erspan`
	Shows the source interface configuration for ERSPAN. Only supported on the 10000 Switch Series.
	`ipfix`
	Selects ipfix. Configures source interface for IPFIX.
	`http`
	Shows the source interface configuration for HTTP.
	`ntp`
	Shows the source interface configuration for NTP.
	`psm`
	Shows the source interface configuration for PSM. Only supported on the 10000 Switch Series.
	`ptp`
	Shows the source interface configuration for PTP.
	`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.
	`workload_migration`
	Shows the source interface configuration for workload migration. Only supported on the 10000 Switch Series.

`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#
```

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 HPE Aruba Networking 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.
	`ipfix`
	Selects ipfix. Configures source interface for IPFIX.
	`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 the **default** VRF:

```
switch# show ipv6 source-interface all
Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP                 VRF
------------------------------------------------------------------
all                                 1111::2222              default
switch#
```

Displaying all IPv6 source-interface protocol configuration for VRF red:

```
switch# show ipv6 source-interface all vrf red
Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP                VRF
------------------------------------------------------------------
all             1/1/1               2005::2               red
switch#
```

Displaying all IPv6 source-interface protocol configurations for all VRFs:

```
switch# show ipv6 source-interface all all-vrfs
Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP                VRF
------------------------------------------------------------------
all                                 2222::3333            all-vrfs
all                                 1111::2222            default
all             1/1/1               2::2                  red
```

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
```

Command History

Release	Modification
10.13	Added the `dns` protocol parameter.
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):

HPE Aruba Networking Central is the priority agent. If no command is specified for ip source-interface, Central will choose the command automatically if it is reachable on any of the known ports.

```
switch# show running-config
vrf green
ip source-interface tftp interface 1/1/2 vrf green
ip source-interface radius interface 1/1/2 vrf green
ip source-interface ntp interface 1/1/2 vrf green
ip source-interface tacacs interface 1/1/2 vrf green
ip source-interface dns interface 1/1/2 vrf green
ip source-interface ubt interface 1/1/2 vrf green
ip source-interface central interface 1/1/2 vrf green
ip source-interface all interface 1/1/2 vrf green
ipv6 source-interface tftp 2222::3333 vrf green
ipv6 source-interface radius 2222::3333 vrf green
ipv6 source-interface ntp 2222::3333 vrf green
ipv6 source-interface tacacs 2222::3333 vrf green
ipv6 source-interface ubt 2222::3333 vrf green
ipv6 source-interface central 2222::3333 vrf green
ipv6 source-interface all 2222::3333 vrf green
ip source-interface tftp 10.20.3.1
ip source-interface radius 10.20.3.1
ip source-interface ntp 10.20.3.1
ip source-interface tacacs 10.20.3.1
ip source-interface psm 10.20.3.1
ip source-interface workload_migration 10.20.3.1
ip source-interface erspan 10.20.3.1
ip source-interface ipfix 10.20.3.1
ip source-interface dns 10.20.3.1
ip source-interface ubt 10.20.3.1
ip source-interface central 10.20.3.1
ip source-interface all 10.20.3.1
interface 1/1/1
     no shutdown
     ip address 10.20.3.1/24
interface 1/1/2
     vrf attach greendefault
     ip address 20.1.1.1/24
     ipv6 address 2222::3333/64
interface 1/1/45
     no shutdown
     ip address 100.1.0.1/24
     ipv6 address 1111::2222/64
ip route 100.2.0.0/24 10.20.3.2
switch#
```

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.

Chapter 8
VLANs

VLANs are primarily used to provide network segmentation at layer 2. VLANs enable the grouping of users by logical function instead of physical location. They make managing bandwidth usage within networks possible by:

- Allowing grouping of high-bandwidth users on low-traffic segments
- Organizing users from different LAN segments according to their need for common resources and individual protocols
- Improving traffic control at the edge of networks by separating traffic of different protocol types.
- Enhancing network security by creating subnets to control in-band access to specific network resources

VLANs are generally assigned on an organizational basis rather than on a physical basis. For example, a network administrator could assign all workstations and servers used by a particular workgroup to the same VLAN, regardless of their physical locations.

Hosts in the same VLAN can directly communicate with one another. A router or a Layer 3 switch is required for hosts in different VLANs to communicate with one another.

VLANs help reduce bandwidth waste, improve LAN security, and enable network administrators to address issues such as scalability and network management.

Refer to the Layer 2 Bridging Guide for VLAN configuration and commands.

Chapter 9

Precision Time Protocol (PTP)

PTP is only supported on the HPE Aruba Networking 8325P, 8360, and 9300 Switch Series (R8Z96A model only).

If PTP is configured on MACsec-supported ports, the switch can experience higher jitter or lower PTP accuracy.

Precision Time Protocol (PTP) is defined in the IEEE 1588 standard (Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems). PTP synchronizes clocks in packet-based networks that include distributed device clocks of varying precision and stability. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. PTP is currently employed to synchronize financial transactions, mobile phone tower transmissions, and networks that require precise timing but lack access to satellite navigation signals.

PTP is not supported on EVPN/VXLAN tunnels.

PTP clocks

A PTP network consists of PTP-enabled devices and devices that are not using PTP. The PTP-enabled devices typically consist of clock-aware devices such as ordinary clocks (which are usually single-port end-stations) and one or more grandsource clocks, transparent clocks, and boundary clocks (multi-port L2/L3 time-aware devices).

The basic clock node types include:

Grandsource clock - A grandsource clock is the primary source of time for the downstream devices. This is a device with greater clock quality which may have direct access to a reference clock.

Ordinary clock - An ordinary clock is a single port end-station (which can include a GM as the originating PTP time-aware device).

Transparent clock (8360 Switch Series only) - A transparent clock can have multiple network port connections but it does not act as either a clock-source or a clock-sink. Rather, it updates the correction field within the PTP event messages (**SYNC/FOLLOW_UP**, **DELAY_REQUEST**) to compensate for the transit time delay. Transparent clocks compensate for switch latency and jitter, making network devices appear transparent to other PTP time-aware devices. They help in reducing the end-station time errors and improving synchronization quality. But a transparent clock itself does not synchronize its time.

There are two types of transparent clocks:

- **End-to-End (E2E) transparent clock**—Updates the **correctionField** field in the PTP messages with the total time the PTP packet was resident in the network device. This is called resident time correction.
- **Peer-to-Peer (P2P) transparent clock**—Updates the **correctionField** field in the PTP messages with the sum of upstream link delay and the resident time. The upstream link delay is the estimated packet propagation delay between the upstream neighbor P2P clock and the local transparent clock.

Boundary clock—The boundary clock implements a local PTP clock where one port will act as clock-sink which synchronizes itself with the clock-source while other ports act as clock-source ports to its downstream clock-aware devices. The clock-source port is used to redistribute the clock to another set

of clock-sinks. The best master clock algorithm (BMCA) is used by the boundary clock to select the best configured acceptable clock-source clock.

Best master clock algorithm

The BMCA behavior changes per profile, but is usually similar to the specified in IEEE 1588-2008 section 9.3.

The clocks broadcast information about their properties (the datasets), which is then used as an input to the selection process. These are the values used in the BMCA, sorted by descending order of preference, as in IEEE 1588-2008:

1. **grandmasterIdentity**: If two datasets suggest the same GM, the one with the least hops, the lower clockIdentity or the lower portIdentity will be chosen. This shall return an error if using a loopback connection.
2. **priority1**: An absolute priority that can be configured by the user (this value is fixed to 128 in G.8275.1 and G.8275.2).
3. **clockClass**: Attribute defining a clock's TAI traceability, synchronization state and expected performance.
4. **clockAccuracy**: Attribute defining the local accuracy of a clock.
5. **offsetScaledLogVariance**: An attribute defining the stability of a clock.
6. **priority2**: User-configurable priority that can be used as a tiebreaker when the other attributes match.
7. **clockIdentity**: A final tiebreaker consisting of the MAC address of the clock.

In all the inputs, the lower number is preferred, e.g. a clock with a priorty1 value of 90 is better than 100. The algorithm runs periodically, so that the device reacts quickly to any attribute changes.

The IEEE 1588 standard allows for an alternate BMCA, which can be used in cases where the default algorithm presents problems or would not suffice the requirements of the network.

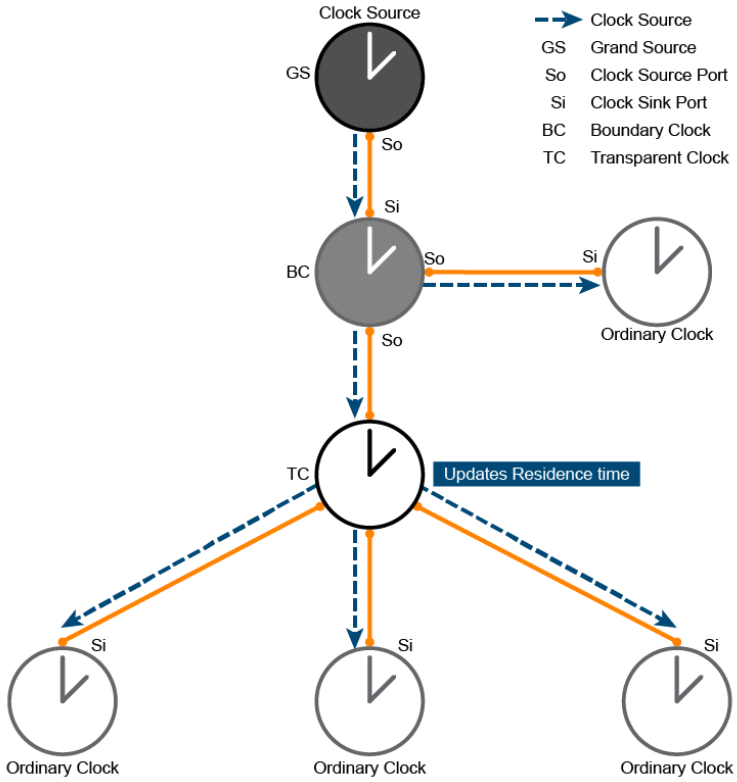
The ITU-T G.8275.1-2022 section 6.3.7 and G.8275.2-2022 section 6.7.9 specify their own alternate BMCA, considering a localPriority value, which is currently non-configurable, therefore it is set to the recommended default of 128. The way the grandmasterIdentity and clock class are used as tiebreakers differs against IEEE 1588 too.

The BCMA is now called the Best timeTransmitter Clock Algorithm (BTCA) on newer revisions of the ITU-T standards.

PTP network diagram

The following diagram illustrates how the various PTP clock nodes are connected and how the timing information flows from the origin to the end-stations to achieve the time synchronization. This diagram depicts the PTP clocks in a source-sink hierarchy.

Figure 1 *Example PTP network with clocks in a source-sink hierarchy*



Configuration examples

Configuring an end-to-end transparent clock (TC E2E)

Follow these steps to configure the E2E transparent clock:

1. Configure the mandatory commands:
    a. Configure the PTP mode and the delay mechanism.
    b. Configure the PTP clock-step mode.
    c. Configure the transport protocol.
    d. Configure PTP globally.

```
Switch config:
switch(config)# ptp profile aes67
switch(config-ptp)# mode transparent end-to-end
switch(config-ptp)# clock-step one-step
switch(config-ptp)# transport-protocol ip
switch(config-ptp)# enable
```

2. Enable PTP on the connected interfaces :

```
switch(config)# int 1/1/1
switch(config-if)# ptp enable
switch(config-if)# int 1/1/2
switch(config-if)# ptp enable
```

Configuring an end-to-end boundary clock (BC E2E)

Follow these steps to configure the end-to-end boundary clock:

1. Create the PTP context using the specified profile.

```
switch(config)# ptp profile aes67
```

2. Configure the mandatory commands:
   a. Configure the PTP mode.
   b. Configure the PTP clock-step mode.
   c. Configure the transport protocol.
   d. Configure PTP globally.

```
switch(config-ptp)# mode boundary end-to-end
switch(config-ptp)# clock-step one-step
switch(config-ptp)# transport-protocol ip
switch(config-ptp)# enable
```

3. Configure the optional commands which participate in the best clock source algorithm:
   a. Configure priority1 value.
   b. Configure priority2 value.

```
switch(config-ptp)# priority1 1
switch(config-ptp)# priority2 10
```

4. Enable PTP on the connected interfaces:

```
switch(config)# int 1/1/1
switch(config-if)# ptp enable
switch(config-if)# int 1/1/2
switch(config-if)# ptp enable
```

5. Optional: changing packet interval rate for various PTP parameters:

```
switch(config-if)# ptp sync-interval 1588v2 1
switch(config-if)# ptp announce-interval 1588v2 -5
switch(config-if)# ptp announce-timeout 1588v2 4
switch(config-if)# ptp delay-req-interval 1588v2 -3
```

PTPv1 passthrough

Only supported on the 8360 Switch Series.

As part of the PTPv1 passthrough feature, PTPv1 packets are allowed to pass through both PTP and non-PTP aware devices. PTPv1 traffic is forwarded based on the destination MAC address and the switches do not process or route the PTPv1 traffic.

As per the IEEE standard, PTPv1 packets are expected to have a TTL value of 0, which makes them operational only in LAN environment and non-routable.

PTP support over VSX

Only supported on the 8360 Switch Series.

PTP Transparent Clock is supported on VSX and supports both P2P and E2E delay mechanisms. The PTP-TC clock configuration is synchronized between VSX peers.

- PTP must be enabled and configured on the Inter Switch Link (ISL) so that the PTP packets bridged through the ISL have the correction field (CF) updated. In case of peer-to-peer (P2P) delay mechanism, the link-delay for the ISL is also determined by the PTP protocol and compensated in the CF.
- PTP for a keepalive (KA) link depends on L3 configuration. If the routing protocol is configured to forward PTP packets through a KA link, then PTP must be enabled on the KA link. In general, it is not recommended to send L3 routed packets through a keepalive link.

Missing SyncE clock source

SyncE is only supported on the 8325P Switch Series.

When a device loses connection with a SyncE clock source there will be a transitional period while the algorithm selects a new clock source from the available options. During this period (typically not more than a few seconds) the QL of the device and devices synchronized downstream may change to an unexpected value. If new clock source is selected, then the final state will show the QL of the new selected source. If there are no other suitable sources the device will move to holdover state and track the internal clock or local oscillator.

Limitations, conflicts, and exclusions

On 8360 Switch Series:

- Peer-to-peer transparent clock requires the clock-domain configuration for the peer-delay packets exchange, whereas the end-to-end transparent clock operates across domains. So the clock-domain configuration is not considered for end-to-end transparent clock.
- With peer-to-peer delay-mechanism (especially two-step), having more than one end client on the same link is not a valid configuration. It is recommended to have only 1:1 peer-to-peer communication.
- If peer-delay packets are made to transit any intermediate nodes (eg. through unicast config or intermediate L2 node, etc.) then it can have higher noise due to non-compensated resident time.
- With IPv4, ECMP is not supported on PTP BC.
- When PTP is disabled on a port, the switch behaves as PTP unaware device. The forwarding rules applicable on the port will take effect based on the transport protocol and the port configuration for the incoming PTP messages.
- When software downgrade is performed from 10.15 and above to versions lower than 10.15, ptp vlan configuration will not be retained. Users need to configure ptp vlan manually again after downgrade.

On the 8325P and 9300 Switch Series:

- Unicast and multicast configurations conflict. In the case where both are configured on the system, unicast will be used and multicast will be ignored.

- To use multicast transmission, all unicast configuration must be removed. If Unicast and multicast are configured together, all Multicast ports will have their states set to Disabled, with the PTP fault reason "Unicast - Multicast configuration conflict". An WARN event log will also be displayed:

```
PTP Unicast and Multicast are both configured. Only Unicast will be honored. If
Multicast operation is desired, remove all PTP Unicast configuration.
```

- When conflicting configurations are entered via CLI, the user will be warned via a printed message. In the case of a unicast port being configured when there are multicast ports configured, the following message will be displayed:

```
Warning: PTP Unicast is configured on this interface, but there are still PTP
Multicast ports configured. PTP Multicast ports will not work until all 'ptp peer
ip' configurations are removed.
```

- In the case of a multicast port being configured when there are Unicast ports configured, the following message will be displayed:

```
Warning: PTP is not operational on this interface.Configure 'ptp peer ip' or
remove all other 'ptp peer ip' configuration to make it operational.
```

- Transparent mode and two-step clock can be configured via REST but are not supported.

The following are not supported on the 8325P, 8360, and 9300 Switch Series:

- IPv6 support
- SMPTE mixed mode

The following are not supported on the 8325P and 9300 Switch Series:

- Peer-to-peer mode
- Transparent clock mode
- Two step option for Clock step.
- VSX/VSF is not supported along with PTP on this platform.
- Only default VRF is supported.
- Multicast and Unicast ports in the same configuration.

On the 8325P and 9300 Switch Series:

- PTP configurations require restarting the PTP service to apply, which can affect the PTP operation at system level and the PTP setting at port level.The following PTP configurations are the only exceptions:
  - Priority1 and Priority2 setting for profile
  - PTP VLAN setting at port level.

On the 8325P Switch Series:

- SyncE configurations require restarting the SyncE service to apply, which can affect the SyncE operation to reconverage based on the wait-to-restore timer configured. The downstream device can also be affected until the system is fully converged.

- LAG membership reconfiguration with SyncE configuration also requires the SyncE service to restart. If a port without any SyncE configuration is assigned to a LAG, it doesn't affect the SyncE service.
- Disable RS-FEC on the PTP enabled 25G port to maintain Class C performance. The 25GbE port with RS-FEC enabled may cause a higher PTP timestamp error. Additionally, enabling and disabling adjacent ports (with RS-FEC) increases the timestamp error and may generate a latency change.
- RS-FEC must be disabled on peer device also to establish link. Configuring the RS-FEC setting will bounce the port.
- Mirroring on egress is not supported for any packets transmitted for CPU. Do not use mirror to capture PTP protocol packets on egress. Mirror PTP protocol packets on ingress is supported.

Hardware considerations

PTP is supported on breakout cables. PTP connections through a QSA28 (QSFP28 to SFP adapter) transceivers are not supported. DACs are not supported for use through QSA28 adapters. (Refer to the *Transceiver Guide* for further information.)

PTP Clients connected to 1 Gbps XCVRs on an 8360 Switch acting as the PTP boundary clock or PTP transparent clock will have a slightly higher offset when there is background data traffic between clients. This is a known limitation specifically to Clients connected only on 1 Gbps links on the HPE Aruba Networking8360 Switch Series. Clients connected on higher speed links (10/25/40/50/100) Gbps will not be impacted.

If PTP is configured on MACsec-supported ports, the switch can experience higher jitter or lower PTP accuracy.

Configuration recommendations

PTP CoPP class configuration recommendations

Configuration recommendations for a boundary clock

The PTP CoPP class must be adjusted based on the number of clients associated with the boundary clock and the configured packet rate. For example, if there are 1000 clients with a configured packet rate of 2pps, and a default CoPP limit of 1000, packet drops will be observed. In such instances the CoPP limit should be increased to more than 2000.

The `show copp statistics class ptp` command can be used to monitor whether the CoPP policy must be adjusted. For example:

```
Statistics for CoPP policy 'default':
Class: ptp
Description: Precision Time Protocol (PTP) .
    priority             : 5
    rate (pps)           : 1000
    burst size (pkts)    : 250

    packets passed   : 611153             packets dropped  : 0
```

Increasing the PTP CoPP values may help in scaling the clients but needs to be planned and configured properly so as to not to impact other protocols.

QoS prioritization configuration recommendations for a transparent clock

```
class ip PTP
    10 match udp any any eq 319 count
policy PTP-POL
    10 class ip PTP action local-priority 6
policy test
interface lag 240
    apply policy PTP-POL in
interface 1/1/26
    apply policy PTP-POL in
interface 2/1/26
    apply policy PTP-POL in
```

PTP Event messages carrying a critical timestamp use UDP port 319.

General guidelines for PTP IPv4 multicast

- For IP multicast-based PTP time distribution, it is recommended to use PIM Sparse-Mode.
- When connecting transparent clock (TC) and boundary clock (BC), ensure that the TC becomes the DR by setting the DR priority.
- Ensure the mroutes are programmed on TCs so that there is reachability for PTP streams from the upstream.
- Configure static-igmp groups on TCs if the clients themselves cannot send IGMP joins for the PTP multicast group.
- The `QoS trust dscp` command needs to be explicitly configured on all non-BC switches in the network to ensure that the incoming DSCP value of PTP traffic is honored.
- If Peer-to-Peer (P2P) does not happen with the immediate peer (for example some configurations with Unicast mode that skip over intermediate-nodes, which could be one or more Transparent Clocks) the offsets may go high.
- Transparent clock peer-to-peer using IPv4 transport requires source IP configuration to send IPv4 PTP messages over L2 MCLAG.

Expected behavior of PTP with VSX (boundary clock)

1. **PTP global disable or interface-level configuration events** - Disabling PTP globally on one of the VSX devices may result in increased offset values, depending on the PTP packet exchange path. The affected device operates as a non-PTP-aware node, which can lead to higher offsets or loss of synchronization until PTP is re-enabled.
2. **PTP interface disable/enable on MCLAG interfaces** - When PTP is disabled on an MCLAG interface of one VSX device, the PTP daemon stops processing PTP packets. As a result, the handling of multicast PTP packets (L2 or L3) depends on the underlying multicast behavior. The device effectively becomes PTP-unaware, potentially causing offset variations in downstream clients. Normal synchronization resumes once the PTP configuration is re-enabled.
3. **PTP configuration mismatch between VSX peers** - If the PTP configurations between VSX peers are inconsistent (e.g., differences in profile, clock-step, clock-mode, or transport-mode), the system behavior can become unpredictable. Each device may process PTP packets differently, leading to unstable offsets and inconsistent synchronization across the network.
4. **VSX ISL flap events (ISL shut/unshut)** - When the VSX ISL is shut, offset values typically remain stable, with only minor spikes lasting a few seconds depending on the PTP tree convergence.

After unshutting the ISL and restoring MCLAG connectivity, brief offset spikes may occur during PTP reconvergence between VSX devices. These stabilize shortly thereafter.

5. **VSX keepalive (KA) flap events (with ISL down and split-recovery disabled)** - During a VSX Keepalive flap with the ISL down and split-recovery disabled, downstream PTP clients generally maintain stable offsets. However, the VSX Secondary device becomes unsynchronized from the Grandmaster (GM) and operates as a standalone PTP device, affecting the synchronization of clients connected to it.
6. **VSX software upgrade events** - When both VSX devices are synchronized with the Grandmaster, performing a software upgrade using the vsx-swupdate command exhibits the following behavior:
   a. During secondary reboot: Downstream client offsets remain stable or experience minor spikes that settle within a few seconds.
   b. During primary reboot: Downstream client offsets remain largely unaffected or show minimal spikes, which stabilize quickly.
   c. Post-reboot and link restoration: Once the Primary device and MCLAGs are operational, brief offset spikes may occur during PTP reconvergence, similar to the ISL recovery scenario.
7. **VSX common system MAC configuration** - Configuring a common system MAC on VSX may momentarily cause an offset spike due to an ISL flap. Despite this, MCLAGs remain operational even when the ISL is down. The offset stabilizes once the VSX Secondary shuts its MCLAGs.

Unsupported/not-Supported PTP and VSX configurations

Both VSX devices must have identical PTP configurations, including PTP clock-mode, PTP clock-step, PTP transport-mode, and PTP profile. If the PTP configurations between the VSX peers differ, the PTP+VSX functionality will not operate as intended. The PTP daemon will verify if the peer VSX device has the same PTP clock-mode (BC).

In a negative scenario, disabling PTP on one VSX device (which was previously receiving PTP Announce and Sync packets from the upstream) while keeping it enabled on the other can lead to unpredictable behavior. However to ensure that the VSX secondary device receives and processes upstream packets through a PTP-unaware VSX primary device, the ISL PTP VLAN must match the upstream PTP VLAN. If the ISL PTP VLAN does not align with the upstream PTP VLAN, the VSX secondary device will drop the received PTP packets without processing them.

PTP on VSX keepalive interface

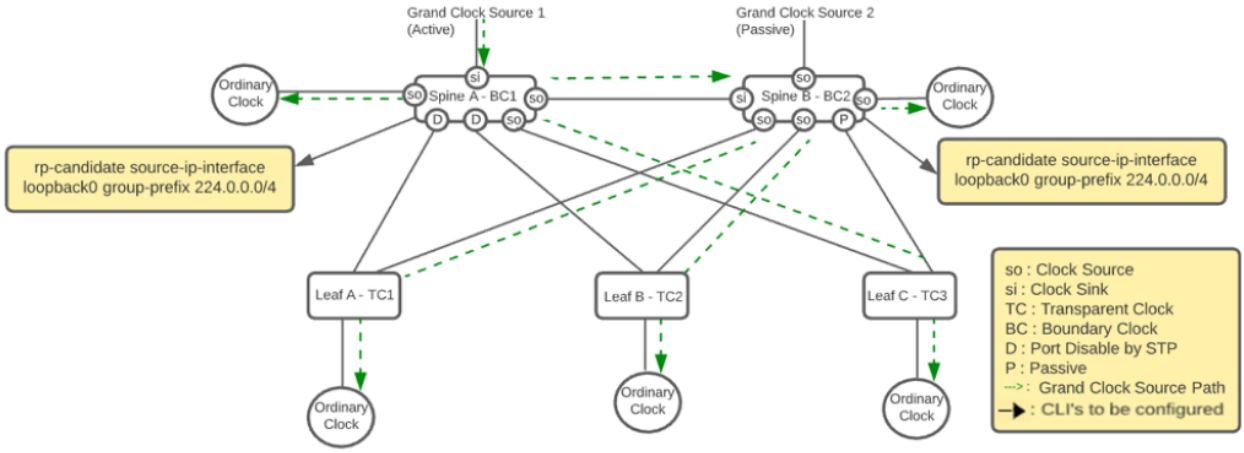
PTP configuration on keepalive interfaces are recommended only on non-OOBM interfaces. PTP is not supported on OOBM interfaces as they do not allow PTP configurations. PTP on keepalive remains disabled even though PTP is configured on KA as long as VSX ISL is active and in sync with VSX Peer. PTP on keepalive will be enabled only when the VSX ISL interface is disabled and remains in shutdown state.

Use cases

The following use cases are only supported on the 8360 Switch Series.

Use case: PTP – IPv4 over L2 spine leaf topology

Figure 1 *Grand clock source connected to boundary clock (spines), followed by transparent clock leaves*



The following considerations and best practices apply to this use case illustrated in the above topology:

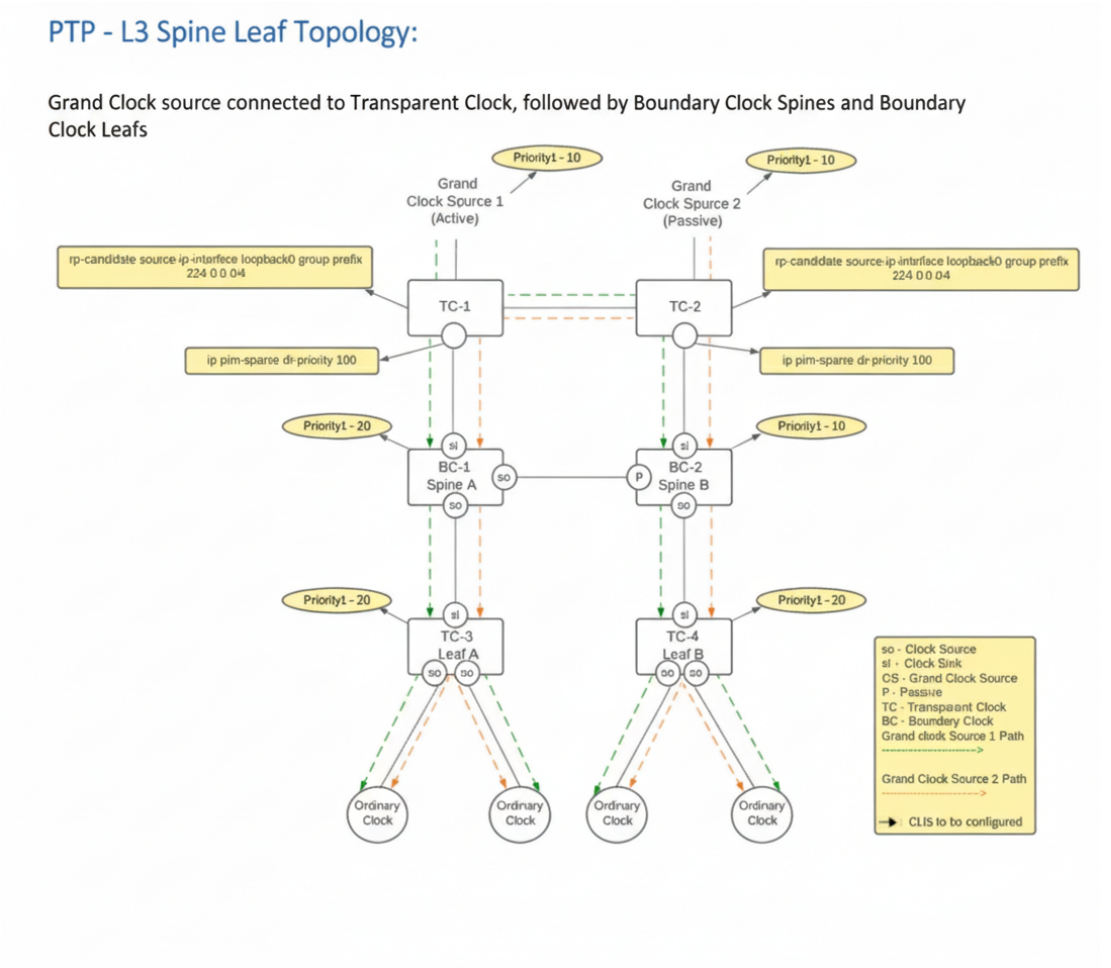
- Configure candidate-RP on switches that are connected to a grand clock source. The candidate-RP needs to be configured on the BC1 Spine A and BC2 Spine B.
- When the PTP clients are not capable of sending IGMP joins, be sure to configure **ip igmp static-group 224.0.1.129** on the VLAN interface of a TC, where PTP is configured.

In this case, it is an L2 switch in leaf so `ip igmp snooping enable` also needs to be configured on the transparent clock VLAN interface.

- Ensure that **ip source-interface ptp** is configured on both BC switches on the VLAN interface where PTP is configured.
- Ensure that **spanning tree** is enabled to avoid unwanted loops.
- In this use case topology, It is recommended to have VRRP on boundary clock switches to have L3 redundancy for PTP end clients.

Use case: PTP – L3 spine leaf topology

Figure 1 *Grand clock source connected to transparent clock, followed by boundary clock spines and boundary clock leaves*

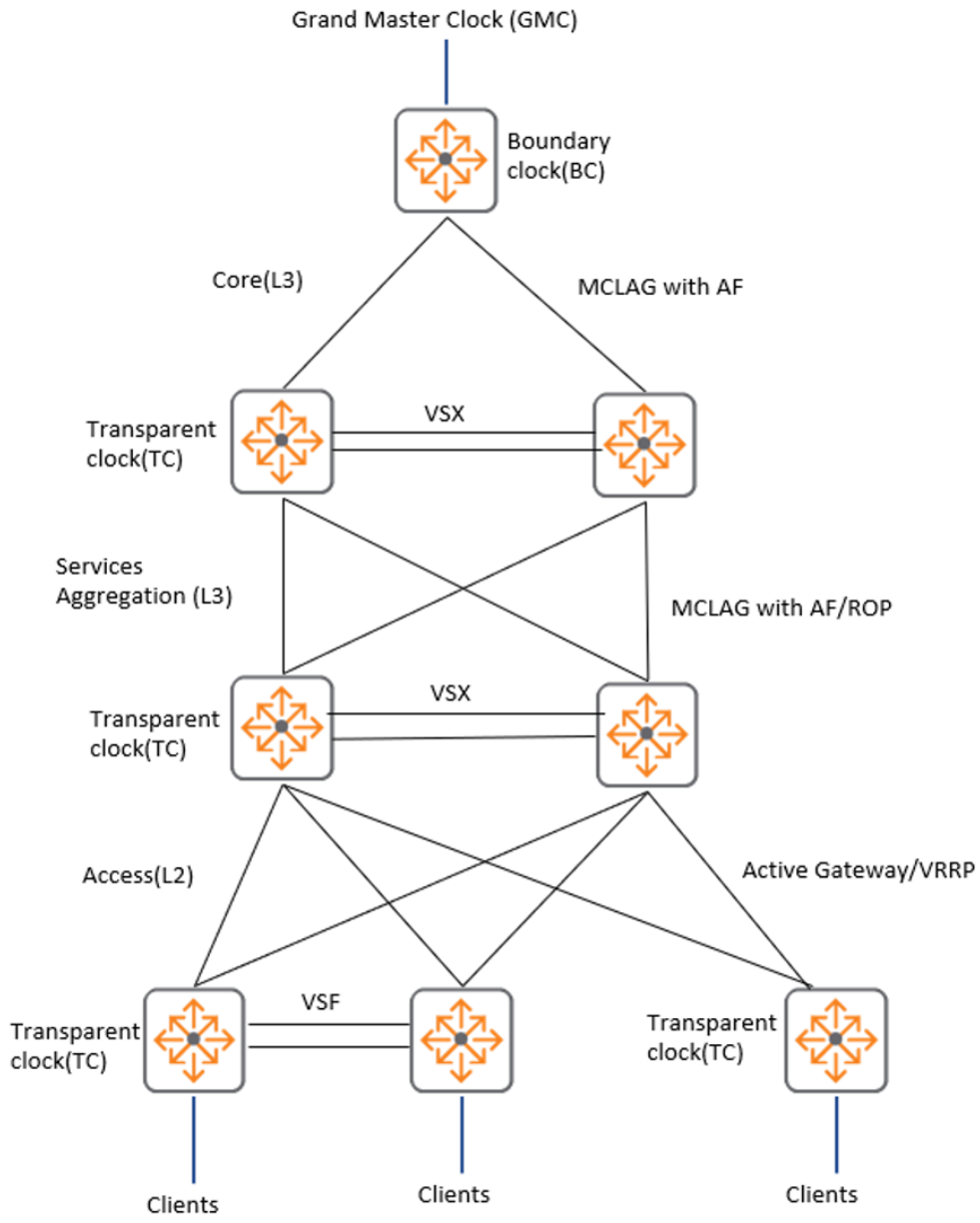


The following considerations and best practices apply to this use case illustrated in the above topology:

- Configure candidate-RP on switches which are connected to a grand clock source. Candidate-RP needs to be configured on TC1 and TC2. Each candidate-RP controls multicast traffic forwarding for one or more multicast groups.
- Configure higher DR priority on switches in which candidate-RP is configured. The DR priority needs to be configured on the TC1 and TC2 on the BC facing ports.
- When the PTP clients are not capable of sending IGMP joins, ensure that **ip igmp static-group 224.0.1.129** is configured on all PTP-enabled interfaces of a TC.
- The **igmp static-group** configuration is not needed on BC switches. In this case, it is an L3 network so **ip igmp enable** also needs to be configured on all PTP-enabled L3 interfaces of the TC.

Use case: PTP-VSX Multicast

Figure 1 *Medium or Large campus solutions for PTP-VSX multicast*



The following considerations and best practices apply to the use case illustrated in the above topology.

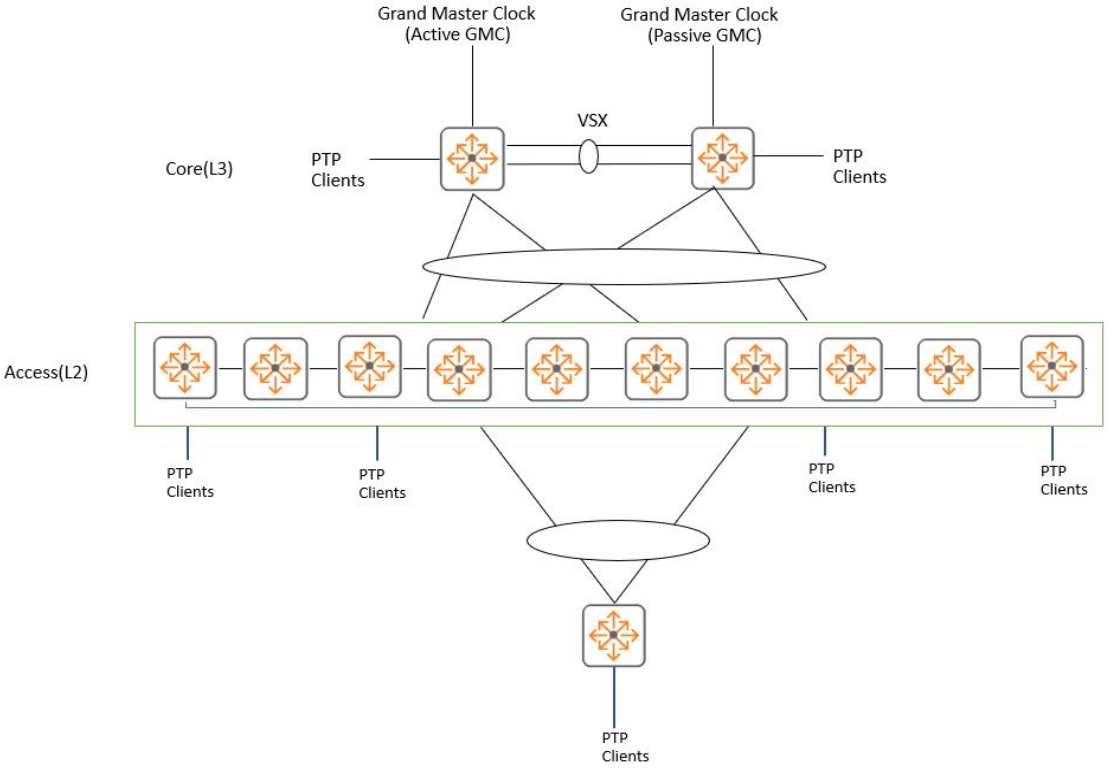
- If there are no dynamic IGMP joins for the PTP Group on the Grand Master Clock (GMC)/client-connected port on the core Boundary Clock (BC), use the command **igmp static group** to configure an IGMP static groups on those ports.
- When a core switch is acting as a Boundary Clock, it is always recommended to use Multi-Chassis Link Aggregation (MC-LAG) with active forwarding as an upstream solution.

In the above topology, if there is a requirement to use ECMP upstream solutions in VSX, the upstream switch should be configured as Transparent Clock (TC).

Use case: PTP TC VSX, BC VSF Topology connected via MCLAG

This recommendation is to address deployments where multicast config change is not feasible and with the help of ACLs unwanted PTP multicast packets can be avoided hitting the PTP BC and overwhelming the PTP CoPP limit.

Figure 1 *VSX TC and VSF topology with clients on VSX and VSF*



1. In the above sample topology, it is possible that multicast PTP delay request from the PTP clients connected to VSX TC which is intended only to the GM may get replicated to the downstream VSF PTP BC as well if the general multicast routing is configured in such fashion.
2. If there are multiple clients on the VSX layer and those clients are in different VLANs, then it may create a multicast storm of PTP messages reaching the BC.
3. To protect the CPU from being overwhelmed, the PTP BC's COPP module will start dropping the excessive PTP messages.
4. The CoPP drops on the BC would cause Announce/Sync/Delay-resp messages from the GM also to get dropped and may result in loss of Synchronization of BC and its PTP clients.
5. In such cases, it is recommended to change the IP multicast configuration to avoid these unwanted PTP packets getting forwarded to the BC. Alternatively, configure ACLs to drop the packets reaching the BC.
6. If the configuration changes listed above are not feasible then alternatively the CoPP limit for PTP can be increased from the default CoPP value after considering the CoPP resource utilization of other features configured in the switch.

Sample ACL configuration

In VSF BC, igmp snooping ACLs can be configured to avoid advertisement of downstream IGMP VLANs towards the VSX.

```
 access-list ip ptp_control
  10 deny any 224.0.1.129 any count
  20 permit any any any

  vlan 52
      ip igmp snooping enable
  vlan 53
      ip igmp snooping enable
      ip igmp snooping apply access-list ptp_control
```

In the VSX TC, ACLs can be applied on all the multicast source destination PTP clients to be dropped on the MCLAG.

```
access-list ip ptp_control
  8 deny any 49.49.49.0/255.255.0.0 224.0.1.129
  9 deny any 51.51.51.0/255.255.0.0 224.0.1.129
  10 deny any 52.52.52.0/255.255.0.0 224.0.1.129
  20 deny any 53.53.53.0/255.255.0.0 224.0.1.129
  100 permit any any any

interface lag 1 multi-chassis
apply access-list ip ptp_control out
```

The ACLs and multicast configuration recommendations are only for reference and may differ for different deployments. Behavior is not specific to VSF and VSX topology and can be seen in any other topology as well as with standalone BC switches.

PTP commands

clear ptp statistics

```
clear ptp statisctics [<IFNAME>]
```

Description

Clears PTP counters for the given interface.

Parameter	Description
<IFNAME>	Optional: Specifies the interface name.

Examples

Clearing PTP counters for the given interface:

```
switch# clear ptp statistics 1/1/8
switch# clear ptp statistics lag1
switch# clear ptp statistics
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Administrators or local user group members with execution rights for this command.

clock-domain

```
clock-domain <DOMAIN-NUMBER>
no clock-domain <DOMAIN-NUMBER>
```

Description

Configures the PTP clock domain to a specified value.

The **no** form of this command removes the PTP domain configuration of the PTP clock.

Parameter	Description
<DOMAIN-NUMBER>	Sets the PTP clock domain. Range: 0 to 254. Value configurable subject to limits established by the PTP profile.

Usage

- The one-step end-to-end transparent clock works across domains.
- For boundary clocks, the clock-domain has to be identical with the domain used in the network.
- All PTP devices must be within same domain to be able to sync with each other.
- This command is only enabled in the PTP profile context.
- For PTP transparent clock, you must configure the same clock-domain as on clients and GM to synchronize.

Examples

Entering the PTP profile context and setting the PTP clock domain value:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)#clock-domain 4
```

Removing the PTP clock domain value:

```
switch(config-ptp)# no clock-domain
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-ptp`	Administrators or local user group members with execution rights for this command.

clock-step

```
clock-step {one-step|two-step}
no clock-step {one-step|two-step}
```

Description

Configures the clock step mode that determines when the egress-time information is sent.

The 8325P and 9300 Switch Series only support the one-step command.

The 8360 Switch Series supports both one-step and two-step modes for boundary clocks. For transparent clocks, only one-step mode is supported.

The **no** form of this command removes the PTP clock-step configuration of the PTP clock.

Parameter	Description
`one-step`	Sets the PTP clock-step mode to one-step messaging in which egress-time information is sent along with the SYNC message.
`two-step`	Sets the PTP clock-step mode to two-step messaging in which egress-time information is sent a subsequent follow-up message with the egress timestamp of the previously sent SYNC message.

Usage

- Mandatory command to start the PTP clock.
- Boundary clocks can inter-operate with different step modes upstream or downstream.

Example

Setting the clock-step mode to one-step messaging:

```
switch(config-ptp)# clock-step one-step
```

Removing the clock-step mode configuration:

```
switch(config-ptp)# no clock-step
```

Setting the clock-step mode to two-step messaging:

```
switch(config-ptp)# clock-step two-step
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-ptp`	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables the PTP profile globally. However, the PTP clock is started only when all the mandatory commands are set.

The **no** form of this command disables the PTP profile globally.

Usage

Mandatory command to start the PTP clock.

Examples

Enabling the PTP profile:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# enable
```

Disabling the PTP profile:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# no enable
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-ptp`	Administrators or local user group members with execution rights for this command.

ip source-interface

```
ip source-interface {ptp | all} interface <IFNAME> [vrf <VRF-NAME>
ip source-interface {ptp | all} <IPV4-ADDR> [vrf <VRF-NAME>]
no ip source-interface {ptp | all} interface <IFNAME> [vrf <VRF-NAME>
no ip source-interface {ptp | all} <IPV4-ADDR> [vrf <VRF-NAME>]
```

Description

Configures the source IP address to be used when sending PTP messages. Use the `ptp` keyword to set source IP address specific to the PTP feature. If the feature-specific configuration is not available, the source IP address corresponding to the `all` option will be used.

The `no` form of this command removes the configuration of the source IP address used by the PTP feature.

Parameter	Description
`ptp`	Selects the PTP protocol.
`all`	Selects all protocols that can be configured by this command.
`interface <IF-NAME>`	Specifies the name of the interface from which the source IP address is obtained. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.
`vrf <VRF-NAME>`	Specifies the VRF name.
`<IPV4-ADDR>`	Specifies the source IPv4 address to be used. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the default VRF, if the vrf option is not used). Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Usage

- This command must be configured on the switch when PTP is enabled on VLAN trunk or access ports, and the transport protocol is IPv4.
- In the current version of PTP, only the default VRF is supported.
- This command is not applicable to the end-to-end transparent clock.

Examples

Configuring the source IP address for sending PTP messages:

```
switch(config)# ip source-interface ptp interface 1/1/1
switch(config)# ip source-interface ptp 10.10.10.1
switch(config)# ip source-interface ptp interface vlan10
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config`	Administrators or local user group members with execution rights for this command.

mode (PTP)

`mode boundary {end-to-end | peer-to-peer}`

```
no mode boundary {end-to-end | peer-to-peer}
mode transparent {end-to-end | peer-to-peer}
no mode transparent {end-to-end | peer-to-peer}
```

Description

Configures the switch PTP clock mode, either boundary or transparent, with a delay-request mechanism of either end-to-end or peer-to-peer. A device in transparent clock mode does not synchronize (syntonize) itself to a grandsource clock. The 9300 and 8325P Switch Series support the **mode boundary end-to-end** command only.

The **no** form of this command unconfigures the PTP clock mode and delay-request mechanism.

Parameter	Description
`boundary`	Selects boundary clock mode.
`transparent`	Selects transparent clock mode.
`end-to-end`	Selects the end-to-end delay-request mechanism.
`peer-to-peer`	Selects the peer-to-peer delay-request mechanism. Not supported with VSF.

Examples

Configuring PTP boundary clock mode with the end-to-end delay-request mechanism:

```
switch(config-ptp)# mode boundary end-to-end
```

Unconfiguring PTP boundary clock mode with the end-to-end delay-request mechanism:

```
switch(config-ptp)# no mode boundary end-to-end
```

Configuring PTP boundary clock mode with the peer-to-peer delay-request mechanism:

```
switch(config-ptp)# mode boundary peer-to-peer
```

Unconfiguring PTP boundary clock mode with the peer-to-peer delay-request mechanism:

```
switch(config-ptp)# no mode boundary peer-to-peer
```

Configuring PTP transparent with the end-to-end delay-request mechanism:

```
switch(config-ptp)# mode transparent end-to-end
```

Unconfiguring PTP transparent with the end-to-end delay-request mechanism:

```
switch(config-ptp)# no mode transparent end-to-end
```

Configuring PTP transparent with the peer-to-peer delay-request mechanism:

```
switch(config-ptp)# mode transparent peer-to-peer
```

Unconfiguring PTP transparent with the peer-to-peer delay-request mechanism:

```
switch(config-ptp)# no mode transparent peer-to-peer
```

Command History

Release	Modification
10.15	Added support for mode boundary end-to-end on the 8325P.
10.14.1000	Added support for mode boundary end-to-end on the 9300.
10.11	Added support for the peer-to-peer delay-request mechanism.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-ptp`	Administrators or local user group members with execution rights for this command.

multicast-address

```
multicast-address {forwarding|non-forwarding}
no multicast-address {forwarding|non-forwarding}
```

Description

Sets the multicast Ethernet MAC address used for PTP packets to be forwardable (01:1B:19:00:00:00) or non-forwardable (01:80:C2:00:00:0E) per the ITU G.8275.1 standard.

The **no** form of this command removes the PTP domain configuration of the PTP clock.

This command is only available for the G.8275.1 profile.

Parameter	Description
`forwarding`	Selects forwardable multicast MAC addresses for PTP. Default.
`non-forwarding`	Selects non-forwardable multicast MAC addresses for PTP.

Examples

Selecting forwardable MAC addresses for PTP:

```
switch(config)# ptp profile g.8275.1
switch(config-ptp)# multicast-address forwarding
```

Selecting non- forwardable MAC addresses for PTP:

```
switch(config)# ptp profile g.8275.1
switch(config-ptp)# multicast-address non-forwarding
```

Unconfiguring the multicast ethernet address setting used for PTP packets. This will set the multicast address state to forwarding (the default state):

```
switch(config)# ptp profile g.8275.1
switch(config-ptp)# no multicast-address
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	config-ptp	Administrators or local user group members with execution rights for this command.

priority1

```
priority1 <PRIORITY>
no priority1 <PRIORITY>
```

Description

Configures the PTP clock **priority1** value of the device. This value is operational when the device is in boundary clock mode and participating in the Best Clock Source Algorithm (BMCA). This value is used to indicate priority to its downstream clock-aware devices.

Priority 1 is fixed as 128 on the 8325P when using the G.8275.1 or G.8275.2 profile and is not configurable.

The **no** form of this command removes the PTP **priority1** configuration of the PTP clock and sets it to the default value of 128.

Parameter	Description
<PRIORITY>	Sets the priority value. Default 128.

Usage

This value can be configured only for the boundary clock.

Examples

Configuring PTP priority1 value:

```
switch(config-ptp)# priority1 129
```

Removing PTP priority1 configuration:

```
switch(config-ptp)# no priority1
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series for the 1588v2 and SMPTE profiles.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-ptp`	Administrators or local user group members with execution rights for this command.

priority2

```
priority2 <PRIORITY>
no priority2 <PRIORITY>
```

Description

Configures the PTP clock **priority2** value of the device. This value is operational when the device is in boundary clock mode and participating in the Best Clock Source Algorithm (BMCA). This value is used to indicate priority to its downstream clock-aware devices.

The **no** form of this command removes the PTP **priority2** configuration of the PTP clock and sets it to the default value of 128.

Parameter	Description
<PRIORITY>	Sets the priority value. Default 128.

Usage

This value can be configured only for the boundary clock.

Examples

Configuring PTP `priority2` value:

```
switch(config-ptp)# priority2 129
```

Removing PTP priority2 configuration:

```
switch(config-ptp)# no priority2
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	config-ptp	Administrators or local user group members with execution rights for this command.

ptp announce-interval

```
ptp announce-interval {1588v2 | g.8275.2 | aes67 | aes-r16 | dot1as | smpte} <LOG-SECONDS>
no ptp announce-interval {1588v2| g.8275.2 | aes67 | aes-r16 | dot1as | smpte}
```

Description

Sets the announce message transmit interval on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command removes the announce message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

The g.8275.1 profile doesn't support announce-interval configuration. Its value is fixed to -3.

Parameter	Description
1588v2	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default: 1.
g.8275.2	Specifies the PTP g.8275.2 profile timers. Range: -3 to 0. Default: 0.
aes67	Specifies the PTP AES67 profile timers. Range: 0 to 1. Default: 1.
aes-r16	Specifies the PTP AES-R16 profile timers. Range: 0 to 1. Default: 1.
dot1as	Specifies the PTP 802.1AS profile timers. Range: -6 to 1. Default: 0.
smpte	Specifies the PTP SMTPE profile timers. Range: -3 to 1. Default: 0.
<LOG-SECONDS>	Sets the announce message interval in log seconds.

Switch series	Supported profiles
8325P	1588v2, g.8275.2 , smpte
8360	1588v2, dot1as, aes67, aes-r16, smpte
9300-32D	1588v2, smpte

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP 1588v2 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-interval 1588v2 1
```

Setting the PTP AES67 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-interval aes67 2
```

Removing the PTP AES67 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp announce-interval aes67
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.13	Support extended for 802.1AS profile.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	config-if	Administrators or local user group members with execution rights for this command.

ptp announce-timeout

```
ptp announce-timeout {1588v2|g.8275.1|g.8275.2|aes67|aes-r16|dot1as|smpte} <COUNT>
no ptp announce-timeout {1588v2|g.8275.1|g.8275.2|aes67|aes-r16|dot1as|smpte}
```

Description

Sets the announce message receipt timeout on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command resets the announce message receipt timeout configuration on a PTP-enabled interface and sets a profile-specific default value.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Range: 2-255. Default: 3.
`g.8275.1`	Specifies the PTP g.8275.1 profile timers. Range: 3-255. Default: 3.
`g.8275.2`	Specifies the PTP g.8275.2 profile timers. Range: 2-255. Default: 3.
`aes67`	Specifies the PTP AES67 profile timers. Range: 2-10. Default: 3.
`aes-r16`	Specifies the PTP AES-R16 profile timers. Range: 2-10. Default: 3.
`dot1as`	Specifies the PTP 802.1AS profile timers. Range: 2-255. Default: 3.
`smpte`	Specifies the PTP SMTPE profile timers. Range: 2-10. Default: 3.
<COUNT>	Specifies the number of announcement intervals.

Switch series	Supported profiles
8325P	1588v2, g.8275.1, g.8275.2, smpte
8360	1588v2, dot1as, aes67, aes-r16, smpte
9300-32D	1588v2, smpte

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP 1588v profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-timeout 1588v2
```

Setting the PTP AES67 profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-timeout aes67 4
```

Resetting the PTP AES67 profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)#no ptp announce-timeout aes67
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.13	Support extended for 802.1AS profile.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-if`	Administrators or local user group members with execution rights for this command.

ptp clock-source-only

```
ptp clock-source-only
no ptp clock-source-only
```

Description

Configures the PTP port state to clock_source state. This prohibits the port from entering into a clock_sink or passive state.
The **no** form of this command removes the clock_source state configuration on the port and returns it to normal BMCA operation.

Usage

This can only be configured for the boundary clock.

Examples

Configuring the clock_source only role for the port:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp clock-source-only
```

Removing the configuration of clock_source only role for the port:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp clock-source-only
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-if`	Administrators or local user group members with execution rights for this command.

ptp delay-req-interval

```
ptp delay-req-interval {1588v2 | g.8275.2 | aes67 | aes-r16 | smpte} <LOG-SECONDS>
no ptp delay-req-interval {1588v2 | g.8275.2 | aes67 | aes-r16 | smpte}
```

Description

Sets the delay_req message transmit interval on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command removes the delay_req message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

The g.8275.1 profile doesn't support **delay-req-interval** configuration. Its value is fixed to -4.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default 0.
`g.8275.2`	Specifies the PTP g.8275.2 profile timers. Range: -6 to 1. Default 0.
`aes67`	Specifies the PTP AES67 profile timers. Range: -3 to 1. Default 0.
`aes-r16`	Specifies the PTP AES-R16 profile timers. Range: 0 to 1. Default 0.
`smpte`	Specifies the PTP SMTPE profile timers. -7 to 1. Default -3.
`<LOG-SECONDS>`	Sets the delay_req message interval in log seconds.

Switch series	Supported profiles
8325P	1588v2, g.8275.2, smpte
8360	1588v2, aes67, aes-r16, smpte
9300-32D	1588v2, smpte

Usage

- Use this command for end-to-end (E2E) mode and use command **ptp pdelay-interval** for peer-to-peer mode.
- This command is only for boundary clock.

Examples

Setting the PTP 1588v2 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp delay-req-interval 1588v2 2
```

Removing a PTP 1588v2 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp delay-req-interval 1588v2
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	config-if	Administrators or local user group members with execution rights for this command.

ptp enable

```
ptp enable
no ptp enable
```

Description

Enables PTP on the interface. The **no** form of this command disables PTP on the interface. PTP can be enabled only on physical L2 or L3 interfaces and LAG L2 or L3 interfaces.

Examples

Enabling PTP on a physical interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp enable
```

Disabling PTP on the interface context:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp enable
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-if`	Administrators or local user group members with execution rights for this command.

ptp lag-role

```
ptp lag-role {primary | secondary}
no ptp lag-role {primary | secondary}
```

Description

Configures the PTP role for the member interfaces of a Link Aggregation (LAG) . When there are two or more member interfaces for a LAG, only one link can be configured as primary and only one other link can be configured as secondary. The primary member interface is used for transmitting the PTP packets generated by the boundary clock. When the primary member goes down, the secondary member is used for PTP packet transmission. If both primary and secondary members go down, PTP does not flip over to the other links of the LAG.

The **no** form of this command removes the PTP role configuration for the LAG member interface.

This command is not supported when configured as a transparent clock.

Parameter	Description
`primary`	Sets the primary PTP lag-role for the LAG member interface.
`secondary`	Sets the secondary PTP lag-role for the LAG member interface.

Usage

- LAG roles must be configured for boundary clock.
- For the primary or secondary LAG roles, ensure that the same link ports are configured on both ends of the LAG.

Examples

Setting the primary PTP lag-role for the LAG member interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp lag-role primary
```

Setting the secondary PTP lag-role for the LAG member interface:

```
switch(config)# interface 1/1/2
switch(config-if)# ptp lag-role secondary
```

Removing the PTP lag-role configuration for the LAG member interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp lag-role
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	config-if	Administrators or local user group members with execution rights for this command.

ptp neighbor-propagation-delay-threshold

```
ptp neighbor-propagation-delay-threshold <THRESHOLD-VALUE>
no ptp neighbor-propagation-delay-threshold
```

Description

Configures PTP neighbor propagation delay threshold in nanoseconds.

The **no** form of this command removes the PTP neighbor propagation delay threshold configuration.

Parameter	Description
<THRESHOLD-VALUE>	Sets the PTP neighbor propagation delay threshold in nanoseconds. The supported range is 0-2147483648. Default threshold value: 800 nanoseconds.

Examples

Setting the PTP neighbor-propagation-delay-threshold:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp neighbor-propagation-delay-threshold 200
```

Removing the PTP neighbor-propagation-delay-threshold:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp neighbor-propagation-delay-threshold
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

ptp pdelay-req-interval

```
ptp pdelay-req-interval {1588v2 | aes67 | aes-r16 | dot1as | smpte} <LOG-SECONDS>
no ptp pdelay-req-interval {1588v2 | aes67 | aes-r16 | dot1as | smpte}
```

Description

Sets the **pdelay_req** message transmit interval on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command removes the **pdelay_req** message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

Parameter	Description
1588v2	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default 0.
aes67	Specifies the PTP AES67 profile timers. 0 to 1. Default 0.
aes-r16	Specifies the PTP AES-R16 profile timers. Range: 0 to 1. Default 0.
dot1as	Specifies the PTP 802.1AS profile timers. Range: -6 to 1. Default 0.
smpte	Specifies the PTP SMTPE profile timers. Range: -7 to 1. Default -3.
<LOG-SECONDS>	Sets the delay_req message interval in log seconds.

Switch series	Supported profiles
8360	1588v2, aes67, aes-r16, dot1as, smpte

Usage

- Use this command for peer-to-peer (P2P) mode and use command **ptp delay-interval** for end-to-end (E2E) mode.

Examples

Setting the PTP 1588v2 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp pdelay-req-interval 1588v2 2
```

Removing the PTP 1588v2 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp pdelay-req-interval 1588v2
```

Setting the PTP AES67 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp pdelay-req-interval aes67 1
```

Removing the PTP AES67 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp pdelay-req-interval aes67
```

Setting the PTP smpte profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp pdelay-req-interval smpte 1
```

Removing the PTP smpte profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp pdelay-req-interval smpte
```

Command History

Release	Modification
10.13	Support extended for 802.1AS profile.
10.11	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

ptp peer ip

```
ptp peer ip <IP-ADDRESS>
no ptp peer ip <IP-ADDRESS>
```

Description

Configures destination IP addresses for the interfaces in unicast transmission.

The **no** form of this command removes the PTP destination IP address configuration for the interfaces in unicast transmission.

Unicast and multicast configurations are mutually exclusive. If a unicast port is configured, all multicast ports will cease operating. If multicast transmission is desired no unicast ports can be configured.

Parameter	Description
`ip <IP-ADDRESS>`	Specifies the peer IPv4 address. Syntax: A.B.C.D

Usage

- This command has no effect when configured as a transparent clock.

Example

Configuring `ptp peer ip` on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp peer ip 10.0.0.1
```

Removing `ptp peer ip` on the interface:

```
switch(config-if)# no ptp peer ip 10.0.0.1
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-if`	Administrators or local user group members with execution rights for this command.

ptp peer-to-peer vlan

```
ptp peer-to-peer vlan <VLAN-ID>
no ptp peer-to-peer vlan
```

Description

Configures a VLAN for PTP pdelay messages.

The **no** form of this command removes the VLAN configuration for PTP pdelay messages on a specified port.

According to Telco standard, the insertion of a VLAN tag is not supported on G.8275.1 profiles. Also, the port will be disabled for PTP if the PTP VLAN is misconfigured.

Parameter	Description
<VLAN-ID>	Specifies VLAN as single VLAN ID. Range 1-4094.

Usage

- This configuration has no bearing on only one-step transparent clock end-to-end, but will be configured on peer-to-peer mode.
- In boundary peer-to-peer clock mode, only PTP pdelay packets with PTP peer-to-peer VLAN are processed. PTP pdelay packets from other VLANs are dropped.
- **ptp peer-to-peer vlan** should be configured on interfaces only when the specific VLAN is a trunk/tagged member of that port. This configuration should not be performed on an access port.

Examples

Configuring VLAN 4 for PTP pdelay messages on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp peer-to-peer vlan 4
```

Removing the VLAN configuration for PTP messages:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp peer-to-peer vlan
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

ptp profile

```
ptp profile {<PROFILE NAME>}
no ptp profile {<PROFILE NAME>}
```

Description

Enters the PTP context to configure the PTP profile in which the device will operate. Configure a PTP profile before configuring mode or other profile-specific parameters. The device can be operating in any one profile at a given point of time.

The **no** form of this command removes the PTP profile configuration in which the device will operate. This command clears the PTP profile and all parameters related to that profile.

Parameter	Description
<PROFILE NAME>	Specifies the profile to be used. Profiles include: ■ 1588v2: Specifies the IEEE 1588-2008 profile to be used. ■ aes67: Specifies the IEEE AES67 profile to be used. ■ aes-r16: Specifies the IEEE AES-R16-2016 profile to be used. ■ dot1as: Specifies the IEEE 802.1AS profile to be used. ■ g.8275.1: Specifies the ITU G.8275.1 profile to be used. ■ g.8275.2: Specifies the ITU G.8275.2 profile to be used. ■ smpte: Specifies the IEEE SMPTE-ST-2059-2 profile to be used.

Switch series	Supported profiles
8325P	1588v2, g.8275.1, g.8275.2 , smpte
8360	1588v2, aes-r16, aes67, dot1as, smpte
9300-32D	1588v2, smpte

Usage

Configure PTP profile before configuring mode or other profile-specific parameters.

Example

Configuring PTP profile **1588v2**:

```
switch(config)# ptp profile 1588v2
```

Configuring PTP profile **smpte**:

```
switch(config)# ptp profile smpte
```

Configuring more than one PTP profile:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# exit
switch(config)# ptp profile smpte
switch(config-ptp)#
The existing profile must be removed using the 'no ptp profile' command before
configuring a different profile.
```

Removing the PTP profile:

```
switch(config-ptp)# no ptp profile
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Support added for the 1588v2 and SMPTE profiles on the 9300 Switch Series.
10.13	Support extended for 802.1AS profile.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config`	Administrators or local user group members with execution rights for this command.

ptp sync-interval

```
ptp sync-interval {1588v2 | g.8275.2 | dot1as | aes67 | smpte} <LOG-SECONDS>
no ptp sync-interval {1588v2 | g.8275.2 | dot1as | aes67 | smpte}
```

Description

Sets the sync message transmit interval on a PTP-enabled interface for a specific PTP profile.

The **no** form of this command removes the sync message transmit interval configuration on a PTP enabled interface and sets it to a profile-specific default value.

The g.8275.1 profile doesn't support sync-interval configuration. Its value is fixed to -4.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Range: -6 to 1. Default 0.
`g.8275.2`	Specifies the PTP g.8275.2 profile timers. Range: -6 to 1. Default 0.
`dot1as`	Specifies the PTP 802.1 AS profile timers. Range: -6 to 1. Default -3.
`aes67`	Specifies the PTP AES67 profile timers. Range: -4 to 1. Default -3.
`smpte`	Specifies the PTP SMTPE profile timers. Range: -7 to -1. Default -3
<LOG-SECONDS>	Sets the sync message interval in log seconds.

Switch series	Supported profiles
8325P	1588v2, g.8275.2 , smpte
8360	1588v2, dot1as, aes67, smpte
9300-32D	1588v2, smpte

Examples

Setting the PTP SMPTE sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval smpte -2
```

Setting the PTP 1588v2 sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval 1588v2 -3
```

Setting the PTP AES67 sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval aes67 -2
```

Removing the PTP AES67 sync interval:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp sync-interval aes67
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.13	Support extended for 802.1AS profile.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	config-if	Administrators or local user group members with execution rights for this command.

ptp sync-timeout

```
ptp sync-timeout dot1as <COUNT>
no ptp sync-timeout dot1as
ptp sync-timeout {g.8275.1|g.8275.2} <COUNT>
no ptp sync-timeout {g.8275.1|g.8275.2}
```

Description

Sets the synchronization message receipt timeout on a PTP enabled interface.

The **no** form of this command resets the synchronization message receipt timeout configuration on a PTP-enabled interface and sets a profile-specific default value.

The dot1as profile is supported on the 8360. The g.8275.1 and g.8275.2 profiles are supported on the 8325P.

Parameter	Description
`dot1as`	Specifies the PTP 802.1AS profile timers.
<COUNT>	Specifies the sync timeout count. 6300 and 8360: Range: 2-255. Default: 3. 8325P: Range: 0-255. Default: 5.
`g.8275.1`	Specifies the PTP G.8275.1 profile timers.
`g.8275.2`	Specifies the PTP G.8275.1 profile timers.

Examples

Setting the PTP 802.1 AS profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-timeout dot1as 4
```

Resetting the PTP 802.1 AS profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp sync-timeout dot1as
```

Setting the PTP g.8275.1 profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-timeout g.8275.1 6
```

Resetting the PTP g.8275.1 profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp sync-timeout g.8275.1
```

Command History

Release	Modification
10.15	Support added for the 8325P Switch Series.
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360	`config-if`	Administrators or local user group members with execution rights for this command.

ptp vlan

```
ptp vlan <VLAN-ID>
no ptp vlan <VLAN-ID>
```

Description

Configures a VLAN for PTP messages. It is necessary when the boundary clock port is a VLAN trunk L2 interface (**no routing**).

The **no** form of this command removes the VLAN configuration for PTP messages.

According to Telco standard, the insertion of a VLAN tag is not supported on G.8275.1 profiles. Also, the port will be disabled for PTP if the PTP VLAN is misconfigured.

Parameter	Description
<VLAN-ID>	For the 8325P, 8325H, and 9300 Switch Series: Specifies a VLAN. Range: 1-4094. For the 8360 Switch Series: Specifies VLAN as single VLAN ID, range or list. Range: 1-4094.

Usage

- This configuration has no bearing on only one-step transparent clock end-to-end. **Ptp peer-to-peer vlan** will be configured on transparent clock peer-to-peer mode.
- In boundary clock mode, only PTP packets in PTP VLAN are processed; PTP packets from other VLANs are dropped.
- **ptp vlan** should be configured on interfaces only when the specific VLAN is a trunk/tagged member of that port. This configuration should not be performed on an access port.

Examples

Configuring VLANs 4 and 5 for PTP messages:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp vlan 4,5
```

Configuring VLANs 2 through 5 for PTP messages:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp vlan 2-5
```

Removing the VLAN configuration for PTP messages:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp vlan
```

Command History

Release	Modification
10.17	Multi-VLAN support added.
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325H 8325P 8360 9300	`config-if`	Administrators or local user group members with execution rights for this command.

show ptp clock

```
show ptp clock [vsx-peer]
```

Description

Shows PTP clock-related information.

Parameter	Description
`[vsx-peer]`	Displays VSX peer switch information. (8360 Switches only).

Example

Showing PTP clock information:

```
switch# show ptp clock
PTP Profile                          : 1588v2
PTP Mode                             : boundary
Delay Mechanism                      : end-to-end
Clock Identity                       : 08:00:11:FF:FE:21:E4:46
Network Transport Protocol           : ethernet
Clock Step                           : Two
Clock Domain                         : 0
```

```
Number of PTP Ports                : 2
Priority1                          : 246
Priority2                          : 248

Clock Quality :
  Class                            : 248
  Accuracy                         : 32
  Offset (log variance)            : 16640

Offset From Clock-Source           : +0.000000000  (s)
Mean Delay                         : +0.000000000  (s)
Steps Removed                      : 0
PTP Clock                          : Thu Dec 10 13:21:01.413 2020
```

Showing PTP clock information on an 8325P/8325H switch:

```
switch# show ptp clock
PTP Profile                        : g.8275.2
PTP Mode                           : boundary
Delay Mechanism                    : end-to-end
Clock Identity                     : 08:00:11:FF:FE:21:E4:46
Network Transport Protocol         : ipv4
Clock Step                         : One
Clock Domain                       : 44
Number of PTP Ports                : 1
Priority1                          : 128
Priority2                          : 128

Clock Quality :
  Class                            : 248
  Accuracy                         : 254
  Offset (log variance)            : 65535

Offset From Clock-Source           : +0.000000014  (s)
Mean Delay                         : +0.000000169  (s)
Steps Removed                      : 1
Multicast-Address                  : forwardable
PTP Clock                          : Thu Dec 10 13:21:01.413 2020
```

Showing hardware resource conflicts on an 8325P/8325H switch:

```
switch# show ptp clock
Priority2                          : 128
Fault reason                       : PTP cannot be enabled. Reason: Blocked by
another feature using a shared hardware resource.

Clock Quality :
  Class                            : 0
  Accuracy                         :
  Offset (log variance)            : 0

Offset From Clock-Source           : +0.000000000  (s)
Mean Delay                         : +0.000000000  (s)
Steps Removed                      : 0
PTP Clock                          : Thu Jan  1 00:00:00.698 1970
```

Command History

Release	Modification
10.16	Command introduced on the 8325H and 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8325H 8360 9300 10000	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp foreign-clock-sources

```
show ptp foreign-clock-sources [vsx-peer]
```

Description

Shows the priority1, priority2, class, accuracy, offset-scaled-log-variance (OSLV), and steps removed information for foreign clock-source nodes.

Parameter	Description
`[vsx-peer]`	Displays VSX peer switch information (8360 Switches only).

Example

Showing PTP foreign clock-source information:

```
switch# show ptp foreign-clock-sources
P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-scaled-log-variance, SR=Steps-removed, V=VLAN Identifier

---------- -------------------------------- ------------------------ ---- ---- ---- ---- ------ ---
Interface  Foreign Port ID                  Clock Source ID          P1   P2   C    A    OSLV   SR
---------- -------------------------------- ------------------------ ---- ---- ---- ---- ------ ---
1/1/1      00:fd:45:ff:fe:67:d5:c0(0x0001)  00:50:56:ff:fe:bd:7b:ff  128  128  13   254  65535  2
```

Showing PTP foreign clock-source information when PTP multiple VLANs are configured on a port on the 8360 Switch Series:

```
switch(config)# show ptp foreign-clock-sources
P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-scaled-log-variance, SR=Steps-removed, V=VLAN Identifier

---------- -------------------------------- ------------------------ ---- ---- ---- ---- ------ ---
Interface  Foreign Port ID                  Clock Source ID          P1   P2   C    A    OSLV   SR
---------- -------------------------------- ------------------------ ---- ---- ---- ---- ------ ---
```

```
1/1/7(V-10)   38:10:f0:ff:fe:87:e0:80(0x07da)  38:10:f0:ff:fe:87:e0:80  10   128  248  254  65535  1
1/1/7(V-11)   38:10:f0:ff:fe:87:e0:80(0x07db)  38:10:f0:ff:fe:87:e0:80  10   128  248  254  65535  1
1/1/7(V-9)    38:10:f0:ff:fe:87:e0:80(0x07d9)  38:10:f0:ff:fe:87:e0:80  10   128  248  254  65535  1
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.12	**vsx-peer** parameter introduced on 8360 Switch Series.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp interface

```
show ptp interface [<IFNAME> | profile-data | dot1as | brief | vsx-peer]
```

Description

Shows PTP port-related information.

When PTP is enabled on a VSF stack it is automatically enabled by default on all VSF interfaces.

Parameter	Description
<IFNAME>	Specifies the interface name.
`profile-data`	Shows additional information of the profile.
`dot1as`	Shows port data specific to the 802.1 AS profile.
`brief`	Shows information in a brief format.
`[vsx-peer]`	Displays VSX peer switch information. (8360 Switches only).

Examples

Showing PTP port information when the switch is acting as a transparent clock:

```
switch# show ptp interface 1/1/1
Port Identity                          : 00:00:00:00:00:00:00:00 (0x0000)
Port Number                            : 0
PTP Version                            : 2
PTP Enable                             : Enabled
```

```
PTP Transport                          : ipv4
Port State                             : Disabled
Delay Mechanism                        : peer-to-peer
Announce Interval (log mean)           : 0
Announce Receipt Timeout               : 0
Sync Interval (log mean)               : 0
Sync Timeout                           : NA
Delay Request Interval (log mean)      : NA
Peer Delay Request Interval (log mean) : 0
Mean Path Delay                        : 0 (ns)
switch#

switch# show ptp interface lag20
Port Identity                          : NA
Port Number                            : NA
PTP Version                            : 2
PTP Enable                             : Enabled
Transport of PTP                       : ipv4
Port State                             : NA
Delay Mechanism                        : end-to-end
Announce Interval (log mean)           : NA
Announce Receipt Timeout               : NA
Sync Interval (log mean)               : NA
Sync Timeout                           : NA
Delay Request Interval (log mean)      : N
Peer Delay Request Interval (log mean) : 0
Mean Path Delay                        : 0 (ns)
```

Showing PTP port information when the switch is acting as a boundary clock:

```
switch# show ptp interface 1/1/1
Interface : 1/1/1
Port Identity                          : 88:3a:30:ff:fe:05:c9:80 (port: 0x0002)
Port Number                            : 2
PTP Version                            : 2
PTP Enable                             : Enabled
Transport of PTP                       : ethernet
Port State                             : Clock Source
Delay Mechanism                        : end-to-end
Announce Interval (log mean)           : 0
Announce Receipt Timeout               : 3
Sync Interval (log mean)               : -3
Sync Timeout                           : NA
Delay Request Interval (log mean)      : 0
Peer Delay Request Interval (log mean) : 0
Mean Path Delay                        : 0 (ns)

switch# show ptp interface lag1
Port Identity                          : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                            : 2
PTP Version                            : 2
PTP Enable                             : Enabled
Transport of PTP                       : ipv4
Port State                             : Clock Source
Delay Mechanism                        : end-to-end
Announce Interval (log mean)           : 0
Announce Receipt Timeout               : 3
Sync Interval (log mean)               : -3
Sync Timeout                           : NA
Delay Request Interval (log mean)      : -3
Peer Delay Request Interval (log mean) : 0
```

```
Mean Path Delay                          : 0 (ns)
Primary Interface                        : 1/1/5
Secondary Interface                      : 1/1/6

switch# show ptp interface
Interface lag20:
Port Identity                            : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                              : 2
PTP Version                              : 2
PTP Enable                               : Enabled
Transport of PTP                         : ipv4
Port State                               : Clock Source
Delay Mechanism                          : end-to-end
Announce Interval (log mean)             : 0
Announce Receipt Timeout                 : 3
Sync Interval (log mean)                 : -3
Sync Timeout                             : NA
Delay Request Interval (log mean)        : -3
Peer Delay Request Interval (log mean)   : 0
Mean Path Delay                          : 0 (ns)
Primary Interface                        : 1/1/5
Secondary Interface                      : 1/1/6

Member Interface 1/1/5:
Port Identity                            : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                              : 2
PTP Version                              : 2
PTP Enable                               : Enabled
Transport of PTP                         : ipv4
Port State                               : Running
Delay Mechanism                          : end-to-end
Announce Interval (log mean)             : 0
Announce Receipt Timeout                 : 3
Sync Interval (log mean)                 : -3
Sync Timeout                             : NA
Delay Request Interval (log mean)        : -3
Peer Delay Request Interval (log mean)   : 0
Mean Path Delay                          : 0 (ns)

Member Interface 1/1/6:
Port Identity                            : 00:fd:45:ff:fe:68:f3:00 (port: 0x0003)
Port Number                              : 3
PTP Version                              : 2
PTP Enable                               : Enabled
Transport of PTP                         : ipv4
Port State                               : Not Running
Delay Mechanism                          : end-to-end
Announce Interval (log mean)             : 0
Announce Receipt Timeout                 : 3
Sync Interval (log mean)                 : -3
Sync Timeout                             : NA
Delay Request Interval (log mean)        : -3
Peer Delay Request Interval (log mean)   : 0
Mean Path Delay                          : 0 (ns)

Interface 1/1/15:
Port Identity                            : 00:fd:45:ff:fe:68:f3:00 (port: 0x0001)
Port Number                              : 1
PTP Version                              : 2
PTP Enable                               : Enabled
Transport of PTP                         : ipv4
Port State                               : Clock Sink
```

```
Delay Mechanism                          : end-to-end
Announce Interval (log mean)             : 0
Announce Receipt Timeout                 : 3
Sync Interval (log mean)                 : -3
Sync Timeout                             : NA
Delay Request Interval (log mean)        : -3
Peer Delay Request Interval (log mean)   : 0
Mean Path Delay                          : 0 (ns)
```

Showing PTP port information in a brief format when the switch is acting as a boundary clock:

```
switch# show ptp interface brief
Interface      PTP State
-------------------------
1/1/11         Clock Sink
1/1/12         Clock Source
1/1/15         Clock Source
1/1/16         Clock Source
```

Showing PTP port information of 802.1AS profile:

```
switch# show ptp int 1/1/1 profile-data dot1as
asCapable                        : TRUE
Compute Neighbor RateRatio       : TRUE
Neighbor RateRatio               : 1.2
Compute Neighbor PropDelay       : TRUE
Neighbor Propagation Delay       : 35 ns
PDelay Lost Response Threshold   : 3
Lost Response Threshold Exceeded : FALSE
```

Showing PTP port information in a brief format when the switch is acting as transparent clock:

```
switch# show ptp interface brief
Interface    PTP State
-------------------------
1/1/11       Clock Source
1/1/12       Clock Sink
1/1/13       Passive
```

Showing PTP port information when multiple VLANs for PTP are configured on a PTP-enabled port:

```
switch# show ptp interface 1/1/1
Port Identity                            : 88:25:10:ff:fe:e5:97:80 (port: 0x0001)
Port Number                              : 1
PTP Version                              : 2
PTP Enable                               : Enabled
PTP Transport                            : ethernet
Port State                               : Multi-VLAN mode
Delay Mechanism                          : end-to-end
Announce Interval (log mean)             : 1
Announce Receipt Timeout                 : 3
Sync Interval (log mean)                 : 0
Sync Timeout                             : NA
Delay Request Interval (log mean)        : 0
Peer Delay Request Interval (log mean)   : NA
Mean Path Delay                          : NA
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.13	Support extended for 802.1AS profile on the 8360 Switch Series.
10.12	**vsx-peer** parameter introduced on 8360 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp interface vlan status

`show ptp interface [<IFNAME> | lag <NUM>] vlan status`

Description

Shows the VLAN status information for PTP on a specified port.

Parameter	Description
<IFNAME>	Specifies the interface name.
`lag <NUM>`	Specifies the LAG number.

Examples

Showing PTP VLAN status for all PTP-enabled interfaces:

```
switch# show ptp interface vlan status
Interface 1/1/1:
VLAN      Status
--------------------------
10        Clock Sink
20        Clock Source
Interface 1/1/2:
VLAN      Status
--------------------------
20        Clock Sink
```

Showing PTP VLAN status for port 1/1/1:

```
switch# show ptp interface 1/1/1 vlan status
VLAN      Status
```

```
--------------------------
10        Clock Sink
20        Clock Source
```

Attempting to show PTP VLAN status when PTP has not been enabled on that interface:

```
switch# show ptp interface 1/1/12 vlan status
PTP is not enabled on 1/1/12
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp parent

```
show ptp parent [vsx-peer]
```

Description

Shows parent node information for the PTP device.

Parameter	Description
`[vsx-peer]`	Displays VSX peer switch information (8360 Switches only).

Example

Showing PTP parent node information:

```
switch# show ptp parent
PTP Parent Properties

Parent Clock
---------------------------
Parent Clock Identity                  : 00:00:00:00:00:00:00:01
Parent Port Number                     :  0x0001
Observed Parent Offset (log variance)  : 65535
Observed Parent Clock Phase Change Rate: 2147483647

Grandsource Clock
---------------------------
Grandsource Clock Identity             : 00:00:00:00:00:00:00:01
Grandsource Clock Quality
  Class                                : 6
```

```
  Accuracy                          : 35
  Offset (log variance)             : 0
Priority1                           : 0
Priority2                           : 0
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.12	**vsx-peer** parameter introduced on 8360 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp statistics

```
show ptp statistics [<IFNAME>][vsx-peer]
```

Description

Shows PTP port statistics.

Parameter	Description
<IFNAME>	Optional. Specifies the interface name.
[vsx-peer]	Displays VSX peer switch information. (8360 Switches only).

Examples

Showing PTP port statistics:

```
switch# show ptp statistics

PTP Interface Statistics

                Received Packets    Sent Packets    Discarded Packets    Lost Packets
Interface: 1/1/15
    Announce                    0            1019                    0               0
    Sync                        0            2038                    0               0
    Signaling                   0               0                    0               0
    DelayReq                    0               0                    0               0
    DelayResp                   0               0                    0               0
    FollowUp                    0               0                    0               0
```

```
    PdelayReq               81957          655750                   0               0
    PdelayResp             655750           81957                   0               0
    PdelayRespFollowUp     655749           81957                   0               0
    Management                  0               0                   0               0

                 Received Packets    Sent Packets    Discarded Packets    Lost Packets
Interface: 1/1/16
    Announce                    0            1019                   0               0
    Sync                        0            2038                   0               0
    Signaling                   0               0                   0               0
    DelayReq                    0               0                   0               0
    DelayResp                   0               0                   0               0
    FollowUp                    0               0                   0               0
    PdelayReq               81957          655750                   0               0
    PdelayResp             655750           81957                   0               0
    PdelayRespFollowUp     655749           81957                   0               0
    Management                  0               0                   0               0
```

Showing PTP port statistics for the specified interface:

```
switch# show ptp statistics 1/1/15

PTP Interface Statistics

                 Received Packets    Sent Packets    Discarded Packets    Lost Packets
Interface: 1/1/15
    Announce                    0            1024                   0               0
    Sync                        0            2048                   0               0
    Signaling                   0               0                   0               0
    DelayReq                    0               0                   0               0
    DelayResp                   0               0                   0               0
    FollowUp                    0               0                   0               0
    PdelayReq               81957          655750                   0               0
    PdelayResp             655750           81957                   0               0
    PdelayRespFollowUp     655749           81957                   0               0
    Management                  0               0                   0               0
```

Showing PTP statistics when PTP multiple VLANs are configured on a port:

```
switch# show ptp statistics

PTP Interface Statistics

                      Received Packets    Sent Packets    Discarded Packets    Lost
Packets
Interface: 1/1/1 Vlan Id: 10
    Announce                     23146              13                    0
      0
    Sync                         23146              25                    6
      0
    Signaling                        0               0                    0
      0
    DelayReq                         0           23141                    0
      0
    DelayResp                    23141               0                    0
      0
    FollowUp                         0               0                    0
      0
    PdelayReq                        0               0                    0
```

```
      0
    PdelayResp                      0               0                0
      0
    PdelayRespFollowUp              0               0                0
      0
    Management                      0               0                0
      0
Interface: 1/1/1 Vlan Id: 20
    Announce                        0           11582                0
      0
    Sync                            0           23164                0
      0
    Signaling                       0               0                0
      0
    DelayReq                    23142               0                0
      0
    DelayResp                       0           23142                0
      0
    FollowUp                        0               0                0
      0
    PdelayReq                       0               0                0
      0
    PdelayResp                      0               0                0
      0
    PdelayRespFollowUp              0               0                0
      0
    Management                      0               0                0
      0
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.12	**vsx-peer** parameter introduced on 8360 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Administrators or local user group members with execution rights for this command.

show ptp statistics vlan

`show ptp statistics [<IFNAME>] vlan <VLAN-ID>`

Description

Shows statistics for PTP VLANs.

Parameter	Description
<IFNAME>	Optional. Specifies the interface name.
<VLAN-ID>	Specifies VLAN as single VLAN ID. Range 1-4094.

Examples

Showing PTP statistics on interface 1/1/1 for VLAN 10:

```
switch# show ptp statistics 1/1/1 vlan 10

PTP Interface Statistics

                     Received Packets    Sent Packets    Discarded Packets    Lost Packets
Interface: 1/1/1 Vlan Id: 10
    Announce                    23146              13                    0               0
    Sync                        23146              25                    6               0
    Signaling                       0               0                    0               0
    DelayReq                        0           23141                    0               0
    DelayResp                   23141               0                    0               0
    FollowUp                        0               0                    0               0
    PdelayReq                       0               0                    0               0
    PdelayResp                      0               0                    0               0
    PdelayRespFollowUp              0               0                    0               0
    Management                      0               0                    0               0
```

Command History

Release	Modification
10.17	Command introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Administrators or local user group members with execution rights for this command.

show ptp time-property

```
show ptp time-property [vsx-peer]
```

Description

Shows PTP clock-time properties for the PTP device.

Parameter	Description
`[vsx-peer]`	Displays VSX peer switch information. (8360 Switches only).

Example

Showing PTP clock time properties:

```
switch # show ptp time-property
PTP Clock Time Property
---------------------------
Current UTC Offset Valid  : FALSE
Current UTC Offset        : 37
Leap59                    : FALSE
Leap61                    : FALSE
Time Traceable            : FALSE
Frequency Traceable       : FALSE
PTP Timescale             : FALSE
Synchronization Uncertain : FALSE
Time Source               : 160
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.12	**vsx-peer** parameter introduced on 8360 Switch Series.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show running-config ptp

```
show running-config ptp
```

Description

Shows PTP running configuration related information.

Example

Showing PTP running configuration information:

```
switch# show running-config ptp
ptp profile smpte
    enable
    clock-step two-step
    transport-protocol ipv4
    mode boundary peer-to-peer
interface 1/1/15
    no shutdown
    ip address 30.1.1.1/16
    ptp enable
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

transport-protocol

```
transport-protocol {ethernet | ip | udp <UDP-PORT>}
no transport-protocol
```

Description

Sets the transport protocol for PTP packets. In the case of IPv4, the UDP check-sum is reset. There is no default transport-protocol.

The **no** form of this command disconnects the clock from its source.

Parameter	Description
`ethernet`	Specifies the Ethernet (Layer 2) transport protocol.
`ip`	Specifies the IPv4 transport protocol.
`udp`	Specifies the UDP transport protocol.
<UDP-PORT>	Specifies the transport layer port. Range: 1-65355. The default is 4739.

Usage

Mandatory command to start the PTP clock.

Example

Setting the Ethernet transport protocol for PTP packets:

```
switch(config-ptp)# transport-protocol ethernet
```

Removing the transport protocol for PTP packets:

```
switch(config-ptp)# no transport-protocol
```

Setting the transport protocol for exporter-1 to UDP with port 2055:

```
switch(config)# flow exporter exporter-1
switch(config-flow-exporter)# transport udp 2055
```

Command History

Release	Modification
10.15	Command introduced on the 8325P Switch Series.
10.14.1000	Command introduced on the 9300 Switch Series.
10.14	Replaced the **ipv4** parameter with the **ip** parameter. The **ipv4** parameter is deprecated.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
8325P 8360 9300	`config-ptp`	Administrators or local user group members with execution rights for this command.

vsx-sync ptp-global

```
vsx-sync ptp-global
no vsx-sync ptp-global
```

Description

Enables synchronization of Precision Time Protocol (PTP) configuration on the VSX peer switch.

The **no** form of this command disables the synchronization of PTP configuration on the VSX peer switch. However, this will not delete the existing PTP configuration on the peer switch.

Examples

Enabling VSX synchronization for PTP configuration:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# mode transparent end-to-end
switch(config-ptp)# exit
switch(config)# vsx
switch(config-vsx)# vsx-sync ptp-global
```

Disabling VSX synchronization for PTP configuration:

```
switch(config)# vsx
switch(config-vsx)# no vsx-sync ptp-global
```

Command History

Release	Modification
10.12	Command introduced.

Command Information

Platforms	Command context	Authority
8360	`config-vsx`	Administrators or local user group members with execution rights for this command.

SyncE commands

esmc enable

```
esmc enable
no esmc enable
```

Description

Configures the interface as a Synchronous Ethernet port by enabling the ESMC protocol for this interface.

The interface is configured to behave as a clock source by default, meaning that it is able to receive ESMC messages and will be considered in the SyncE clock selection process according to the ESMC protocol. The interface will not transmit ESMC messages. Before enabling ESMC on an interface, it must be assigned a unique priority. Refer to synce priority for additional SyncE clock source priority configuration information.

When an interface is configured to receive ESMC it will continuously monitor for the reception of ESMC packets. The packets are expected at a rate of 1 per second (as specified in ITU-T G.8264). If the interface stops receiving ESMC packets for more than 5 seconds, it will enter the "Rx timeout" condition and its current quality level will be set to QL-FAILED.

The **no** form of the command disables the Synchronous Ethernet feature on an interface.

Examples

Enabling SyncE on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# esmc enable
```

Disabling SyncE on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no esmc enable
```

Attempting to enable SyncE on an interface prior to configuring **synce priority**:

```
switch(config)# interface 1/1/1
switch(config-if)# esmc enable
Unique priority must be configured before enabling ESMC on interface
```

```
switch(config-if)# synce priority 1
switch(config-if)# esmc enable
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	config-if	Administrators or local user group members with execution rights for this command.

esmc transmit-only

```
esmc transmit-only
no esmc transmit-only
```

Description

Configures the interface as a Synchronous Ethernet transmit-only mode interface. This means that the interface is not capable of receiving ESMC messages or running the ESMC protocol and will not be considered in the clock selection process. Instead, the interface will send ESMC packets advertising the current quality level of the system. Initial quality level cannot be configured on a transmit-only interface. The synce priority can be configured but will be active only if the mode is rx/tx. When operating in tx-only mode, the value will remain configured but inactive.

The **no** form of the command resets the interface to Synchronous Ethernet clock source mode. This means that the interface will receive and process ESMC messages but will not transmit them. The interface will also be eligible for the clock selection process.

All SyncE-configured LAG member ports must be configured with same operation mode, either transmit or receive. Mixing operation modes on different LAG member ports is not supported.

Examples

Configuring interface 1/1/1 as transmit-only mode interface:

```
switch(config)# interface 1/1/1
switch(config-if)# esmc transmit-only
```

Resetting interface 1/1/1 to SyncE clock source mode:

```
switch(config)# interface 1/1/1
switch(config-if)# no esmc transmit-only
```

Configuring a priority on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# synce priority 2
```

Attempting to configure an initial quality level on an interface that has been configured as transmit-only:

```
switch(config)# interface 1/1/1
switch(config-if)# synce initial-quality-level PRC
Cannot configure initial quality level on transmit-only interface 1/1/1
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	config-if	Administrators or local user group members with execution rights for this command.

show synce interface

`show synce interface [{<IFNAME> | brief}]`

Description

Shows the current status of selected quality level, selected port name, selected clock index, SyncE DPLL state, and holdover remaining time.

The rank is a value used internally to select the best SyncE source. It is composed as follows, in hexadecimal:
0x AA BB CC
AA = Quality level, BB = Priority, and CC = Number of hops. The lower the rank, the better the source.

Parameter	Description
<IFNAME>	Specifies an interface name.
brief	Specifies interface brief.

Examples

Showing an individual SyncE interface status:

```
switch# show synce interface 1/1/1
Status                      : Enabled
ESMC Mode                   : Receive
Clock State                 : Qualified
Sync State                  : Normal
Current Quality Level       : ePRTC
```

```
Priority                    : 11
Rank                        : 0x000B01
Number of Hops              : 1
Rx Status                   : Active
```

Showing the status of all interfaces with SyncE enabled:

```
switch# show synce interface
Interface: 1/1/1
Status                      : Enabled
Clock State                 : Qualified
Sync State                  : Normal
ESMC Mode                   : Receive
Current Quality Level       : PRC
Configured Quality Level    : SSUA
Priority                    : 4
Rank                        : 0x031602
Number of Hops              : 2
Rx Status                   : Active

Interface: 1/1/2
Status                      : Enabled
ESMC Mode                   : Transmit

Interface: 1/1/12
Status                      : Enabled
ESMC Mode                   : Receive
Priority                    : Not set
Rank                        : Not available
Rx Status                   : Inactive

Interface 1/1/22:
Status                      : Enabled
ESMC Mode                   : Receive
Clock Index                 : 8
Clock State                 : Qualified
Sync State                  : Normal
Current Quality Level       : FAILED
Priority                    : 22
Rank                        : 0x3E1601
Number of Hops              : 1
Rx Status                   : Timed out
ESMC Mode                   : Receive
Clock State                 : Qualified
Sync State                  : Normal
Current Quality Level       : FAILED
Priority                    : 22
Rank                        : 0x3E1601
Number of Hops              : 1
Rx Status                   : Timed Out
```

Showing SyncE brief interface status:

```
switch# show synce interface brief
Interface    Type         Quality Level     Priority     Rank
-----------------------------------------------------------------
1/1/1        Clock        PRC               2            0x031602
1/1/4        Clock        NCFG              4            None
1/1/2        Transmit     N/A               N/A          N/A
```

Showing SyncE status of interface with SyncE configured but that has been disabled:

```
switch(config)# interface 1/1/5
switch(config-if)# synce priority 10
switch(config-if)# exit
switch(config)# show synce interface 1/1/5
Status                      : Disabled
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	Manager (#)	Administrators or local user group members with execution rights for this command.

show synce status

```
show synce status
```

Description

Displays the current status of selected quality level, selected port name, and the SyncE clock state. When the selected clock source is the internal clock, the selected clock quality is the quality of the internal clock and depends on the network type configured. When the SyncE service is not running such as when there is no port with ESMC enabled or missing configuration, then the clock quality is shown as "N/A".

Network type to internal clock quality mapping:

- Option 1 - QL-SEC
- Option 2 - QL-SMC

Examples

Showing SyncE status where a port has been selected as the clock source and the local clock is synchronized to its corresponding SyncE signal:

```
switch# show synce status
Synchronous Ethernet Status
---------------------------
Selected Clock Quality    : QL-PRC
Selected Clock Source     : 1/1/1
Synchronization State:    : locked
```

Showing SyncE status when the connection to the selected clock was lost but the internal clock is within the holdover period and with the SyncE default network type option 1:

```
switch# show synce status
Synchronous Ethernet Status
```

```
-----------------------------
Selected Clock Quality    : QL-SEC
Selected Clock Source     : Internal clock
Synchronization State     : holdover
```

Showing SyncE status with the SyncE service is running, no clock has been selected, and the SyncE default network type option 1:

```
switch# show synce status
Synchronous Ethernet Status
-----------------------------
Selected Clock Quality    : N/A
Selected Clock Source     : Internal clock
Synchronization State     : freerun
```

Showing SyncE status with the SyncE service running, the synchronization has been lost, the holdover period has expired, and the SyncE default network type option 1:

```
switch# show synce status
Synchronous Ethernet Status
-----------------------------
Selected Clock Quality    : QL-SEC
Selected Clock Source     : Internal clock
Synchronization State     : freerun
```

Showing SyncE status when the SyncE service is not running:

```
switch# show synce status
Synchronous Ethernet Status
-----------------------------
Selected Clock Quality    : N/A
Selected Clock Source     : Internal clock
Synchronization State     : freerun
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	Manager (#)	Administrators or local user group members with execution rights for this command.

synce

```
synce
no synce
```

Description

Enables the synchronous ethernet feature on the device.

The **no** form of the command disables the feature.

Examples

Enabling synchronous ethernet:

```
switch(config)# synce
```

Disabling synchronous ethernet:

```
switch(config)# no synce
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	`config`	Administrators or local user group members with execution rights for this command.

synce hold-off-time

```
synce hold-off-time <MILLISECONDS>
no synce hold-off-time [<MILLISECONDS>]
```

Description

Sets the time in milliseconds for clock source interfaces to be down before beginning new clock selection.

The **no** form of this command resets to the time for clock source interfaces to be down before beginning new clock selection to the default value of 300 milliseconds.

Parameter	Description
<MILLISECONDS>	Time in milliseconds for clock source interfaces to be down before beginning new clock selection. Range: 0-32767. Default: 300.

Examples

Setting the time for clock source interfaces to be down before beginning new clock selection to 400 milliseconds:

```
switch(config)# synce hold-off-time 400
```

Resettting the time for clock source interfaces to be down before beginning new clock selection to the default value of 300 milliseconds:

```
switch(config)# no synce hold-off-time
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	config	Administrators or local user group members with execution rights for this command.

synce initial-quality-level

```
synce initial-quality-level
{ncfg|eprtc|prtc|eprc|prc|ssua|ssub|esec|sec|dnu|prs|stu|st2|tnc|st3e|st3|smc|st4|prov|dus}
no synce initial-quality-level
[{ncfg|eprtc|prtc|eprc|prc|ssua|ssub|esec|sec|dnu|prs|stu|st2|tnc|st3e|st3|smc|st4|prov|dus}]
```

Description

Configures the initial quality level of the clock source interface.

The initial quality level must be valid for the configured network-option, otherwise it will not be applied to the interface. When an initial quality level better than DNU/DUS is configured, it is considered in the initial calculation of rank and port selection. It will effectively be the current quality level of the interface until a different quality level is received from ESMC or the "Rx timeout" condition is hit. If the interface is selected as the best clock source during this transient period, then the switch will advertise this initial quality level as the system current quality level, meaning that a device synchronized downstream will momentarily receive this quality level. If this value is not configured, then the initial quality level for the interface during first rank calculation will be QL-FAILED.

The **no** form of this command removes the configured initial quality level of the clock source interface.

Parameter	Description
ncfg	The quality level is not configured. Default.
eprtc	The timing quality of an enhanced primary reference time clock. Can be configured on either network option-1 or option-2.
prtc	The timing quality of a primary reference time clock. Can be configured on either network option-1 or option-2.
eprc	The timing quality of an enhanced primary reference clock. Can be configured on either network option-1 or option-2.

Parameter	Description
prc	Timing quality of a primary reference clock (option-1 only).
ssua	Timing quality of a type I or IV clock (option-1 only).
ssub	Timing quality of a type VI clock (option-1 only).
esec	The timing quality of an enhanced synchronous equipment clock. Can be configured on network option-1 only.
sec	The timing quality of a synchronous equipment clock. Can be configured on network option-1 only.
dnu	A clock source that should not be used for selection (option-1 only).
prs	Clock traceable to a primary reference source (option-2 only).
stu	Clock not traceable to an known source (option-2 only).
st2	Clock traceable to Stratum 2 (option-2 only).
tnc	Clock traceable to a transit node clock (option-2 only).
st3e	Clock traceable to Stratum 3E (option-2 only).
st3	Clock traceable to Stratum 3 (option-2 only).
smc	Clock traceable to a self-timed SONET clock (option-2 only).
st4	Clock traceable to Stratum 4 free-run (option-2 only).
prov	Clock source provisioned by the network operator. Can be configured on network option-2 only.
dus	A clock source that should not be used for selection (option-2 only).

Examples

Configuring the initial quality level of the clock source interface as primary reference clock:

```
switch(config)# interface 1/1/1
switch(config-if)# synce initial-quality-level prc
```

Configuring the initial quality level of the clock source interface as a type I or IV clock:

```
switch(config)# interface 1/1/1
switch(config-if)# synce initial-quality-level ssua
```

Removing the configured initial quality level of the clock source interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no synce initial-quality-level prs
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	`config-if`	Administrators or local user group members with execution rights for this command.

sync network-type

```
synce network-type {option-1 | option-2}
no synce network-type [{option-1 | option-2}]
```

Description

Sets the network type for the Synchronous Ethernet equipment to optimize for different frequencies.

The **no** form of this command resets the network type to its default setting.

Parameter	Description
`option-1`	Selects Synchronous Ethernet optimization for 2048 Kbps. Default.
`option-2`	Selects Synchronous Ethernet optimization for 1544 Kbps.

Examples

Configuring Synchronous Ethernet frequency type option-1:

```
switch(config)# synce network-type option-1
```

Configuring Synchronous Ethernet frequency type option-2:

```
switch(config)# synce network-type option-2
```

Resetting Synchronous Ethernet frequency type to its default setting:

```
switch(config)# no synce network-type option-1
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	`config`	Administrators or local user group members with execution rights for this command.

synce priority

```
synce priority <PRIORITY>
no synce priority [<PRIORITY>]
```

Description

Sets the priority of the Synchronous Ethernet clock source to use during selection. The priority is the main criterion used for selection if the Quality Level is disabled, or if two clock sources have the same Quality level.

The priority configuration must be unique and no two ports can have the same priority value.

Priority must be configured before enabling ESMC on an interface, unless the interface is configured in transmit-only mode. Priority value 255 is reserved for the local oscillator, which is the selected clock when the system is in holdover state.

The **no** form of this command removes the configured value of the priority for the Synchronous Ethernet clock source and leaves the value as empty. If the SyncE feature was enabled on the interface it will remain enabled, however the interface will not participate in the clock selection process.

All SyncE-configured LAG member ports must be configured with same operation mode, either transmit or receive. Mixing operation modes on different LAG member ports is not supported.

Parameter	Description
<PRIORITY>	Specifies the priority for the Synchronous Ethernet Clock Source to be used in clock selection. Range: 0-254.

Examples

Configuring interface 1/1/1 with a priority of 1:

```
switch(config)# interface 1/1/1
switch(config-if)# synce priority 1
```

Removing the configured priority 1 from interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no synce priority 1
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	`config-if`	Administrators or local user group members with execution rights for this command.

sync quality-mode

```
sync quality-mode
no sync quality-mode
```

Description

Enables Synchronous Ethernet clock selection based on the received quality level of clock sources. Enabled by default.

The **no** form of this command will ignore quality level when selecting a clock source. Selection will be based on the configured priority.

Examples

Enabling SyncE clock selection based on the received quality level of clock sources:

```
switch(config)# sync quality-mode
```

Disabling Synchronous Ethernet clock selection based on quality level of clock sources:

```
switch(config)# no sync quality-mode
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	`config`	Administrators or local user group members with execution rights for this command.

sync wait-to-restore

```
sync wait-to-restore <SECONDS>
no sync wait-to-restore [<SECONDS>]
```

Description

The time in seconds that a Synchronous Ethernet port should remain fault-free to be considered for clock selection.

The **no** form of this command resets the time for Synchronous Ethernet ports to be up before sending ESMC messages to the default value of 60 seconds.

Parameter	Description
<SECONDS>	Time in seconds that a Synchronous Ethernet port should remain fault-free to be considered for clock selection. Range: 0-720. Default: 60.

Examples

Setting the time for Synchronous Ethernet ports to be up before sending ESMC messages to 15 seconds:

```
switch(config)# synce wait-to-restore 15
```

Resetting the time for Synchronous Ethernet ports to be up before sending ESMC messages to the default value of 60 seconds:

```
switch(config)# no synce wait-to-restore
```

Command History

Release	Modification
10.15	Command introduced.

Command Information

Platforms	Command context	Authority
8325P	`config`	Administrators or local user group members with execution rights for this command.

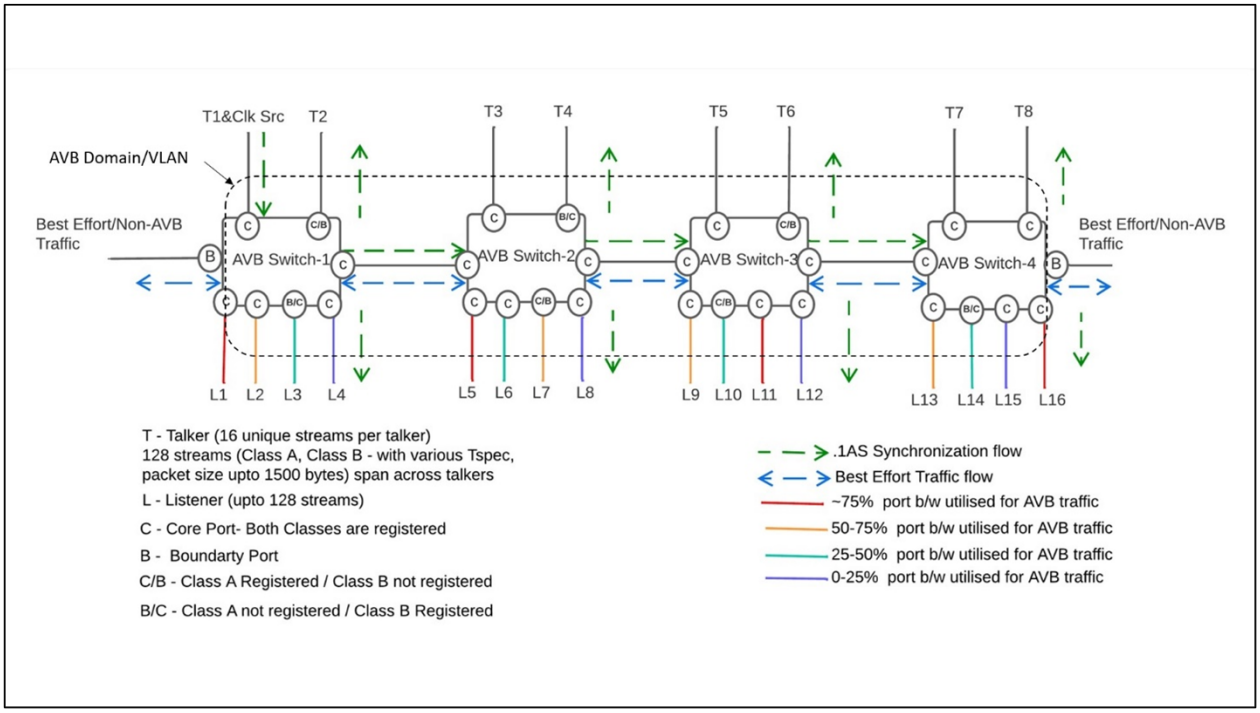
Audio-Video Bridging (AVB)

AVB is supported only on the HPE Aruba Networking 6300 and 8360 Switch Series (JL717C, JL718C, JL721C, JL722C, R8S89A, and R8S90A).

Audio-Video Bridging (AVB) defines features, options, configurations, defaults, protocols, and procedures of bridges, stations, and Local Area Networks (LANs) that are necessary to build networks that are capable of transporting time-sensitive audio and/or video data streams. AVB operates on the concept of stream reservation. Stream Reservation Protocol (SRP) is an amendment to the IEEE 802.1Q standard (standardized separately as 802.1Qat) to provide end-to-end management of resource reservations for data streams requiring guaranteed Quality of Service (QoS) in Local Area Networks (LANs).

AOS-CX switch series support only as AV bridge. AVB is supported only over default STP instance(CIST). AVB is activated through feature-pack.

Figure 1 *Illustrative AVB topology with the validated profile*



Multiple Stream Registration Protocol

Multiple Stream Registration Protocol (MSRP) is a signaling protocol that provides end-stations with the ability to reserve network resources that guarantee the transmission and reception of data streams across a bridged network with the requested QoS. The end stations are referred to as Talkers (devices that produce data streams) and Listeners (devices that consume data streams). MSRP defines payloads and rules for propagating registrations for both Talkers and Listeners. MSRP relies on Multiple Reservation Protocol (MRP) for its communication. MRP (IEEE 802.1Q-2018 section 10) is a robust, efficient protocol for declaring attributes to be registered in a database in each port of each bridge (optionally, station) in a bridged network.

Stream-ID should always be generated from Source MAC of talker and multicast AVB streams are supported. MSRP rank-based prioritization and pre-emption is not supported. MSRP Listener registration is considered when the corresponding talker stream is registered. Streams with non-AVB VLAN are sent as Talker failed with error code 16 (Changes in FirstValue for a registered StreamID). As per protocol functionality, standard failure codes 1, 5, 8, 14, 15, 16, and 19 are generated.

MSRP timer configuration

Whenever MSRP timer config is changed, for the protocol to operate more efficiently, and with less likelihood of unwanted deregistrations, the following relationships should be maintained between timer values used by peer Participants:

- LeaveTime should be at least twice the maximum JoinTime, plus six times the timer resolution, to allow reregistration after a Leave or LeaveAll even if a message is lost.
- To minimize the volume of rejoining traffic generated following a LeaveAll, the value chosen for LeaveAllTime should be large relative to LeaveTime.

Forwarding and queueing for time sensitive streams

Forwarding and Queueing for Time-Sensitive Streams (FQTSS) is an IEEE 802.1Qav standard to describe a set of procedures and tools that can be used to support the forwarding and queueing requirements for AVB.

QoS Configuration

AVB requires the Class-A and Class-B traffic to be given the highest priority and thus manages these class-queues and a control-queue (reserved/future-use). While AVB manages the (3) AVB queues, flexibility is available to customize the mapping of the local-priority to any (5) non-AVB queues. The following is one of the suggested templates for Queue and Schedule profile:

Among the (5) non-AVB queues, queue 4 has highest priority and all protocol control packet (BPDUs) exchange happens in queue 4. So transmitting data traffic at line rate in queue 4 can cause control packet (BPDUs) to get dropped and result in loss of protocol convergence. It is recommended to keep the overall control and data traffic within 25% port speed that are egressing through AVB egress port.

Ensure that the QoS configuration is applied before AVB enablement for proper queueing and bandwidth allocation. It is suggested not to change the Queue-mapping or add conflicting ACLs when AVB is enabled as it can lead to undefined traffic-handling, drops, or affect the latency.

If the user-configured Queue-profile is incorrect when AVB is operational, AVB must be disabled, then the valid 5-Queue profile must be correctly applied, and AVB re-enabled. Do not change the Queue/Schedule profile when AVB is operational. PCP values for class-A and class-B are fixed to 3 and 2, respectively.

The example queue-profile and schedule-profile configuration is given below:

```
switch(config)# qos queue-profile newQprofile
switch(config-queue) # map queue 4 local-priority 7
switch(config-queue) # map queue 4 local-priority 6
switch(config-queue) # map queue 3 local-priority 5
switch(config-queue) # map queue 3 local-priority 4
switch(config-queue) # map queue 2 local-priority 3
switch(config-queue) # map queue 2 local-priority 2
switch(config-queue) # map queue 1 local-priority 1
switch(config-queue) # map queue 0 local-priority 0
switch(config-queue)# exit
switch(config-queue)# qos schedule-profile tmp_msrp-profile
switch(config-schedule)# strict queue 4
switch(config-schedule)# dwrr queue 3 weight 1
switch(config-schedule)# dwrr queue 2 weight 1
switch(config-schedule)# dwrr queue 1 weight 1
switch(config-schedule)# dwrr queue 0 weight 1
switch(config-schedule)#exit
switch(config)# apply qos queue-profile newQprofile schedule-profile tmp_msrp-
profile
```

It is suggested to keep the top user-manageable queue (i.e. Queue-4) as Strict-Priority (SP) to avoid drops in the highest priority non-AVB and control traffic.

AVB caps the maximum reservation to 75% of port bandwidth so that non-AVB traffic is not starved. In case of congestion or over-subscription, the non-AVB traffic >25% is affected in accordance to the user-defined queue-mapping with Queue-0 getting the lowest precedence.

Traffic gets remapped on entering an SRP domain carrying the priority value associated with the domain is forward by the bridge at the domain boundary using a lower priority. Any non-AVB traffic having PCP values 2 and 3 with the same as SRVLAN ID, Cos value is remarked to 0 at the egress.

In case of any replication traffic congestion, packet drops can be seen across the queues/priorities.

Generalized precision time protocol configuration

gPTP (generalized Precision Time Protocol) incorporates the functionality of PTP as defined by IEEE 802.1as, It operates over a LAN network and takes care of timing, synchronization, and PTP functionality requirements over the AVB network.

AVB requires dot1as profile to be configured for its timing and synchronization requirements. If no PTP profile is enabled, enabling AVB enables the dot1as profile internally. If any other PTP profile is configured, AVB enablement fails, the PTP profile must be removed or fixed and AVB must be re-enabled. Removing or disabling the dot1as profile results in AVB going to non-operational.

VLAN configuration

AVB enable internally enables the AVB VLAN if it is not configured. AVB VLAN is a mandatory requirement for the functionality. Removal of AVB VLAN results in AVB going to non-operational. If MVRP is enabled globally, then **AVB enable** does not internally enable the static VLAN and waits for AVB VLAN to be created dynamically. If AVB is enabled first followed by MVRP, then the static VLAN is already created by **AVB enable**. In this scenario, AVB continues to operate with the static VLAN. Manually remove the AVB static VLAN using **no vlan** if dynamic creation of AVB VLAN (through MVRP registration) is expected.

Feature exclusions

- AVB supports static or dynamic (based on MVRP registration) AVB VLAN configuration and only one AVB VLAN is supported.
- User should not configure the following for AVB:
  - LAG
  - VSF
  - VSX (ISL and MCLAGs)
  - Split cables
  - MTU, EEE, Flow control

AVB commands

avb

```
avb
no avb
```

Description

Enables the AVB feature and creates the AVB context. Enables user to exercise various configuration options available under AVB.

The **no** form of this command removed the AVB configuration in the global context.

Examples

Enable AVB:

```
switch(config)# avb
switch(config-avb)#
```

Disable AVB:

```
switch(config)# no avb
AVB configuration will be deleted.
Continue (y/n)? y
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

clear msrp statistics

```
clear msrp statistics [<IF-NAME>]
```

Description

Clears the MSRP counters for the given interfaces.

Parameter	Description
<IFNAME>	Specifies the interface name.

Examples

Clear the MSRP counter for interface 1/1/1:

```
switch# clear msrp statistics 1/1/1
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables AVB globally.
The **no** form of this command disables AVB globally.

Examples

Enable audio video bridging:

```
switch(config)# avb
switch(config-avb)# enable
```

Disable audio video bridging:

```
switch(config)# avb
switch(config-avb)# no enable
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	`config`	Administrators or local user group members with execution rights for this command.

max fan in ports

```
max-fan-in-ports <NUMPORTS>
no max-fan-in-ports <NUMPORTS>
```

Description

Configures the AVB maximum number of fan in ports globally. The default maximum is 10. Whenever the max-fan-in-ports is changed, AVB disable and enable are required to make it operational.
The **no** form of this command sets the AVB maximum number of fan in ports to default.

Parameter	Description
<NUMPORTS>	Specifies the maximum number of fan in ports. Range: 1-10. Default: 10.

Examples

Enable AVB max-fan-in-ports 3:

```
switch(config)# avb
switch(config-avb)# max-fan-in-ports 3
Disable and Enable AVB to reflect max-fan-in-ports configuration as operational.
```

Disable AVB VLAN 3 max-fan-in-ports and setting to default:

```
switch(config)# avb
switch(config-avb)# no max-fan-in-ports 3
Disable and Enable AVB to reflect max-fan-in-ports configuration as operational.
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	config	Administrators or local user group members with execution rights for this command.

msrp

```
msrp
no msrp
```

Description

Configures the MSRP protocol on the interface
The **no** form of this command disables the MSRP protocol on the interface.

Examples

Enable MSRP protocol on the interface:

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

Disable MSRP protocol on the interface:

```
switch(config-if)# no msrp
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

msrp timer join

```
msrp timer join <TIME-INTERVAL>
no msrp timer join <TIME-INTERVAL>
```

Description

Configures the MSRP join timer on a MSRP enabled interface. The timer configures the time to wait for the MSRP Protocol Data Units (PDUs) to be sent out of the interface. The timer units are in centiseconds. The default is 20 centiseconds.
The **no** form of this command sets the configuration back to the default value.

Parameter	Description
<TIME-INTERVAL>	Specifies the time interval in centiseconds. Range: 20-100. Default: 20.

Examples

Configure MSRP timer join to 50 centiseconds:

```
switch(config-if)# msrp timer join 50
```

Remove MSRP timer join configuration and set to default timers:

```
switch(config-if)# no msrp timer join 50
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

msrp timer leave

```
msrp timer leave <TIME-INTERVAL>
no msrp timer leave <TIME-INTERVAL>
```

Description

Configures the MSRP leave timer on a MSRP enabled interface. The timer configures the time to wait for the MSRP registrar state to move from LEAVE state to EMPTY state on the interface. The timer units are in centiseconds. The default is 300 centiseconds.
The **no** form of this command sets the configuration back to the default value.

Parameter	Description
<TIME-INTERVAL>	Specifies the time interval in centiseconds. Range: 40-1000000. Default: 300.

Examples

Configure MSRP timer leave to 500 centiseconds:

```
switch(config-if)# msrp timer leave 500
```

Remove MSRP timer leave configuration and set to the default configuration:

```
switch(config-if)# no msrp timer leave 500
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	`config-if`	Administrators or local user group members with execution rights for this command.

msrp timer leaveall

```
msrp timer leaveall <TIME-INTERVAL>
no msrp timer leaveall <TIME-INTERVAL>
```

Description

Configures the MSRP leaveall timer on a MSRP enabled interface. The timer configures the time to wait for the leaveall messages to be sent on the interface. The timer units are in centiseconds. The default is 1000 centiseconds.
The **no** form of this command sets the configuration back to the default value.

Parameter	Description
<TIME-INTERVAL>	Specifies the time interval in centiseconds. Range: 500-1000000. Default: 1000.

Examples

Configure MSRP leaveall timer to 500 centiseconds:

```
switch(config-if)# msrp timer leaveall 500
```

Remove MSRP leaveall timer configuration and set to default configuration:

```
switch(config-if)# no msrp timer leaveall 500
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	config-if	Administrators or local user group members with execution rights for this command.

show avb domain

```
show avb domain
```

Description

Displays the global AVB domain status.

Examples

Display the global AVB domain status:

```
switch# show avb domain
AVB state                          : operational
AVB VLAN                           : 2
Max Fan in Ports                   : 10
AVB Class-A
        Priority Code Point        : 3
        Number of Core Ports       : 1
        Number of Boundary Ports   : 1
AVB Class-B
        Priority Code Point        : 2
        Number of Core Ports       ; 1
        Number of Boundary Ports   : 1
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show avb interface

```
show avb interface [<IFNAME> | brief]
```

Description

Displays the AVB interface information.

Parameter	Description
<IFNAME>	Specifies the interface name.
brief	Shows information in brief format.

Examples

Display the AVB interface status:

```
switch# show avb interface 1/1/2
AVB state                          : Enabled
MSRP State                         : Enabled
PTP State                          : Enabled, asCapable
  Neighbor Propogation Delay       : 98
  Port State                       : clock_source
  Peer Mean Path Delay             : 99
AVB readiness state                : operational
Allocated BW (Kbit/s)              : 7500000
Used BW (Kbits/s)                  : 27456
Available BW (Kbits/s)             : 7472544
Per-class value                    Class-A                 Class-B
-------------------------------------------------------------------
Tx srClassVID                      2                       2
Rx srClassVID                      2                       2
Tx PCP                             3                       2
Rx PCP                             3                       -
Domain State                       Core                    Boundary
```

Display the AVB interface status in brief:

```
switch# show avb interface brief
Ethernet     Peer PCP      Peer    AVB Core       Allocated       Available
Used
Interface    A | B         VLAN    A | B          (Kbit/s)        (Kbit/s)
(Kbit/s)
-------------------------------------------------------------------------------
---------
1/1/1        3 | 2         2       YES | YES      0               0
0
1/1/2        3 | 2         2       YES | NO       7500000         7472544
27456
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show msrp interface

```
show msrp interface [<IFNAME> | brief]
```

Description

Displays MSRP interface information.

Parameter	Description
<IFNAME>	Specifies the interface name.
brief	Shows information in brief format.

Examples

Display the MSRP interface 1/1/1 information:

```
switch# show msrp interface 1/1/1
Stream  Id                : 00:11:01:00:00:01:00:01
Stream  Age               : N/A
Peer Participant         : Talker
Registration Attribute
Type                  : Talker-advertise
Registrar State       : Registered(IN)
Last registered Event : JoinIn
Declaration Attribute
Type                  : Listener-ready
Applicant State       : Quiet Active(QA)
Last Declared Event   : JoinIn
Declared Failure Info : N/A
```

Display the MSRP interface 1/1/2 information in brief:

```
switch# show msrp interface 1/1/2 brief
Stream-Id               Peer        Applicant  Registrar  Reservation
Failure
                        Participant State      State      Status
-------------------------------------------------------------------------------
---------
00:11:01:00:00:01:00:01  Listener    qa         in         Reserved
N/A
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show msrp statistics

```
show msrp statistics [<IF-NAME>]
```

Description

Displays the MSRP statistics for MSRP enabled interfaces.

Parameter	Description
<IFNAME>	Specifies the interface name.

Examples

Display the MSRP interface 1/1/1 statistics:

```
switch# show msrp statistics 1/1/1
Total PDU Transmitted : 7029
Total PDU Received    : 7036
Leaveall Tx count     : 2242
Leaveall Rx count     : 2260
Domain Tx count       : 2242
Domain Rx count       : 4908

               TALKER-ADV    TALKER-FAILED    LISTENER-ASKING-FAILED      LISTENER-READY-FAILED
LISTENER-READY
Rx-New              0              3                       0                         0
      0
Rx-In               0              0                       0                         0
0
Rx-Empty            0              0                       0                         0
      0
Rx-JoinEmpty     6545              0                       0                         0
      0
Rx-JoinIn        7170              0                       0                         0
0
Rx-Leave            3              0                       0                         0
      0
Tx-New              0              0                       2                         0
6
Tx-In               0              0                       0                         0
 0
Tx-Empty            0              0                       0                         0
0
```

```
Tx-JoinEmpty       0             0                  79                  0
   6367
Tx-joinIn          0             0                 105                  0
7170
Tx-Leave           0             0                   0                  0
      3
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show msrp state

`show msrp state <STREAM-ID>`

Description

Displays all information about a given stream.

Parameter	Description
<STREAM-ID>	Specifies the Stream ID.

Examples

Display the MSRP stream information:

```
switch# show msrp state 00:11:01:00:00:01:00:01
Stream-ID           : 00:11:01:00:00:01:00:01
Stream Talker Port  : 1/1/32
Stream Creation time: 1 minute
Destination MAC     : 91:e0:f0:00:fe:00
VLAN                : 2
Priority            : 3 (class-A)
Rank                : low
Accumulated Latency : 20 ns
Max frame size      : 100
Max frame interval  : 1 (frames/125 us)
Bandwidth           : 9152 (Kbit/s)
Status              : active
Failure Information : N/A
Failure Bridge      : N/A
--------------------------------------------------------------------------------
---------
Port    Reg     Appl    Peer          Reg                 Decl                  Rsvn
```

```
       State  State  Participant   Attribute          Attribute
status
-------------------------------------------------------------------------------
---------
1/1/31   in    qa    listener      listener_ready      talker_advertise
Reserved
1/1/32   in    qa    talker        talker_advertise    listener_ready       N/A
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8300	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show msrp streams

```
show msrp streams
```

Description

Displays all information about MSRP streams.

Examples

Display the MSRP stream information:

```
switch# show msrp streams
Stream-Id                DMAC               VLAN  Priority Rank Accumulated
                                                   (class)       Latency
        Bandwidth   Status    Talker Port
        (Kbit/s)
-------------------------------------------------------------------------------
---------
00:11:01:00:00:01:00:01  91:e0:f0:00:fe:00  2     3 (A)   low  150020
        9152        active    1/1/1
00:11:01:00:00:01:00:05  91:e0:f0:00:fe:02  2     3 (A)   low  150020
        9152        active    1/1/1
00:11:01:00:00:01:00:03  91:e0:f0:00:fe:01  2     3 (A)   low  150020
        9152        active    1/1/1

Note: One extra byte (per packet) is considered (to offset the clock diff from the
neighbor device) for MSRP stream bandwidth.
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show msrp streams statistics

```
show msrp streams statistics
```

Description

Displays the traffic statistics for all streams.

Examples

Display the MSRP traffic statistics:

```
switch# show msrp streams statistics
Stream-Id                DMAC               Class     In Packets   Drop Packets
      In Bytes     Drop bytes
-------------------------------------------------------------------------------
---------
00:11:01:00:00:01:00:01  91:e0:f0:00:fe:00  3 (A)              0              0
                0            0
00:11:01:00:00:01:00:05  91:e0:f0:00:fe:02  3 (A)              0              0
                0            0
00:11:01:00:00:01:00:03  91:e0:f0:00:fe:01  3 (A)              0              0
                0            0
Note: The drop counters are pointing to the ACL drops associated to a given
stream.
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators 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 avb

```
show running-config avb
```

Description

Displays all configured commands under the AVB context.

Examples

Display configured commands under the AVB context:

```
switch# show running-config avb
avb
        enable
        vlan 3
        max-fan-in-ports 4
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

vlan

```
vlan <VLAN ID>
no vlan <VLAN ID>
```

Description

Configures the AVB VLAN globally. The default AVB VLAN is 2. Whenever the VLAN is changed, AVB disable and enable are required to make it operational.
The **no** form of this command sets the AVB VLAN to default.

Parameter	Description
<VLAN ID>	Specifies the VLAN. Range: 1-4094. Default: 2.

Examples

Enable AVB VLAN 3:

```
switch(config)# avb
switch(config-avb)# vlan 3
Disable and Enable AVB to reflect VLAN configuration as operational.
```

Disable AVB VLAN 3 and setting to default:

```
switch(config)# avb
switch(config-avb)# no vlan 3
Disable and Enable AVB to reflect VLAN configuration as operational.
```

Command History

Release	Modification
10.13.1000	Featured introduced.

Command Information

Platforms	Command context	Authority
8360	`config`	Administrators or local user group members with execution rights for this command.

Upgrade and downgrade scenarios

Upgrade and downgrade scenarios are provided by the Configuration Migration Framework (CMF).

Upgrades

All upgrade scenarios are supported and configuration is migrated.

Downgrades

The following scenario is supported:
Create a checkpoint before upgrading.
Upgrade.
Perform config changes.
Set the startup configuration to the checkpoint created in step 1.
Downgrade

Configuration changes that occur after the checkpoint in step 1 will be lost during the downgrade.

Limitations

The following are the limitations of upgrade and downgrade scenarios provided by CMF.

Table 1: *Configuration from and to the same build*

From/to	Checkpoint	Running	Startup
Checkpoint	N/A	Supported	Supported
Running	Supported	N/A	Supported
Startup	Supported	Supported	N/A
Config from URL in CLI Format	Supported	Supported	Supported
Config from URL in JSON Format	Supported	Supported	Supported

Table 2: *Configuration from an older build to a newer build (upgrade)*

From/to	Checkpoint	Running	Startup
Config from URL in CLI Format	Not supported	Not supported	Not supported

From/to	Checkpoint	Running	Startup
Config from URL in JSON Format	Not supported	Not supported	Not supported
Startup	Not supported	Supported	Supported

Table 3: *Configuration from a newer build to an older build (downgrade)*

From/to	Checkpoint	Running	Startup
Config from URL in CLI Format	Not supported	Not supported	Not supported
Config from URL in JSON Format	Not supported	Not supported	Not supported
Startup	Not supported	Not supported	Not supported

REST Use Case Examples

The firmware update table contains columns to initiate firmware updates and upload firmware images off the switch. The following columns are used to start these requests:

- src_url
- dst_url
- vrf
- options
- start_request

Supported URL Formats

- Download
  - src_url
    - http://SERVER[:PORT]/FILENAME
    - https://SERVER[:PORT]/FILENAME
    - tftp://SERVER[:PORT][;blocksize=<512-65464>]/FILENAME
  - dst_url
    - flash:/primary
    - flash:/secondary
- Upload
  - src_url
    - flash:/primary
    - flash:/secondary
  - dst_url
    - tftp://SERVER[:PORT][;blocksize=<512-65464>]/FILENAME

- Local image transfer
  - src_url
    - flash:/primary
    - flash:/secondary
    - usb:/file
  - dst_url
    - flash:/primary
    - flash:/secondary
    - usb:/file

If src_url = dst_url an error will be reported and the request will fail.

Firmware Update Options

The options column specifies options that can be configured for firmware transfers.

- https_ca_trust_anchor - Specifies the certificate authority trust store to use when validating the server's certificate. Must be configured when using HTTPS, ignored for other protocols. Possible values are:
  - user - Not currently supported
  - switch - Use the switch's device identity certificates. Used for downloading from another switch via firmware site distribution
  - hpe - Use HPE global file server certificates. Used by Cloud Management for downloading images from the global HPE file server.
  - password - Not currently supported

Additionally, while a firmware transfer is in progress, the status of the transfer can be monitored through the Status column. The following are possible values:

- not_started
- starting
- transferring
- verifying
- complete
- failed
- aborted

The Statistics column can also be monitored to determine information about the update in progress:

- percent_complete
- bytes_total
- bytes_transferred
- time_elapsed
- transfer_rate
- start_time
- finish_time
- estimated_completion_time
- retry_num

start_time and finish_time are stored in seconds since the epoch. time_elapsed indicates the number of seconds since the start of the update. estimated_completion_time indicates the number of seconds until the update is expected to be complete.

After a firmware update has completed, the Status column will either indicate complete, failed, or aborted. A value of complete indicates that the update was completed successfully. In case of a failure, the status will indicate failed and the failure_reason column will be updated to display the reason for the failure.

Failure_reason:

- number
- description

failure_reason.number indicates a numeric value corresponding to the failure reason. failure_reason.description indicates a textual description for the failure. At any time during a firmware update the process may be aborted by writing to the abort_request column. An abort is triggered on an integer value change in this column.

The general execution flow is as follows:

1. Execute a PATCH operation to update the following columns: src_url, dst_url, vrf, options, start_request.
2. A new firmware update will be triggered on any integer value change in the start_request column. A requestor may need to read this value first to ensure that the start_request value being used is different than the current value.
3. During the firmware update transfer, monitor the Status, and Statistics columns using a GET operation. Statistics are updated at 1 second intervals.
4. Monitor the Status column until status indicates completed, failed, or aborted.
5. If the status indicates failed, read the failure_reason column to determine the reason for the failure.

Firmware update transactions can only be processed one at a time. If a new request is received while a current request is in progress it will be ignored. The processed_request column is updated to indicate the request currently in progress. This column will match the value of the start_request used to initiate the update.

Use case 1 - TFTP download

1. Start TFTP download to the primary image location using the management VRF:

```
curl -X PATCH "https://1.1.1.2/rest/v10.17/system/firmware_update" \
  -H "accept: */*" \
  -H "Content-Type: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw==" \
  -d '{
    "src_url": "tftp://1.1.1.10/NL_10_17_0001.swi",
    "dst_url": "flash:/primary",
    "start_request": 1,
    "vrf": "/rest/v10.17/system/vrfs/mgmt"
  }'
```

2. Monitor status, statistics, and processed_request until status shows either complete or failed:

```
curl -X GET "https://1.1.1.2/rest/v10.17/system/firmware_
update?attributes=status,processed_request,statistics" \
  -H "accept: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw=="

**Results**
{
  "processed_request": 1,
  "statistics": {
    "bytes_total": 686059690,
    "bytes_transferred": 26765824,
    "estimated_completion_time": 325,
    "finish_time": 0,
    "percent_complete": 2,
    "retry_num": 0,
    "start_time": 1752786982,
    "time_elapsed": 16,
    "transfer_rate": 2230270
  },
  "status": "transferring"
}

After some time...

curl -X GET "https://1.1.1.2/rest/v10.17/system/firmware_
update?attributes=status,processed_request,statistics" \
  -H "accept: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw=="


**Results**
{
  "processed_request": 1,
  "statistics": {
    "bytes_total": 686059690,
    "bytes_transferred": 686059690,
    "estimated_completion_time": 0,
    "finish_time": 1752787287,
    "percent_complete": 100,
    "retry_num": 0,
    "start_time": 1752786982,
    "time_elapsed": 305,
    "transfer_rate": 2275936
  },
  "status": "complete"
}
```

Use case 2 - Update the secondary firmware image from another switch using firmware site distribution

1. Configure the source switch for firmware site distribution. Please see the firmware site distribution user guide for information on how to configure this feature.
2. Start an HTTPS download to the secondary image location using the switch https_ca_trust_ anchor.

```
curl -X PATCH "https://1.1.1.2/rest/v10.17/system/firmware_update" \
  -H "accept: */*" \
  -H "Content-Type: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw==" \
  -d '{
    "src_url": "https://1.1.1.30:9443/fwimages/primary.swi",
    "dst_url": "flash:/secondary",
    "start_request": 500,
    "vrf": "/rest/v10.17/system/vrfs/mgmt"
    "options": {
      "https_ca_trust_anchor": "switch"
    },
  }'
```

3. Monitor status, statistics, and processed_request until the status is either complete or failed.

```
curl -X GET "https://1.1.1.2/rest/v10.17/system/firmware_
update?attributes=status,processed_request,statistics" \
  -H "accept: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw=="


**Results**
{
  "processed_request": 500,
  "statistics": {
    "bytes_total": 686059690,
    "bytes_transferred": 686059690,
    "estimated_completion_time": 0,
    "finish_time": 1752787287,
    "percent_complete": 100,
    "retry_num": 0,
    "start_time": 1752786982,
    "time_elapsed": 305,
    "transfer_rate": 2275936
  },
  "status": "complete"
}
```

Use Case 3 - Initiate and abort an HTTP transfer

1. Start an HTTP download to the secondary image location using the management VRF

```
curl -X PATCH "https://1.1.1.2/rest/v10.17/system/firmware_update" \
  -H "accept: */*" \
  -H "Content-Type: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw==" \
  -d '{
    "src_url": "http://1.1.1.20/NL_10_17_0001.swi",
    "dst_url": "flash:/secondary",
    "start_request": 100,
    "vrf": "/rest/v10.17/system/vrfs/mgmt"
  }'
```

2. Write to abort_request to abort the update

```
curl -X PATCH "https://1.1.1.2/rest/v10.17/system/firmware_update" \
  -H "accept: */*" \
  -H "Content-Type: application/json" \
  -H "x-csrf-token: Ejq2OIa3z31SGvmK3gyWag==" \
  -d '{
    "abort_request": 100
  }'
```

3. Read status and failure_reason to confirm update is aborted

```
curl -X GET "https://1.1.1.2/rest/v10.17/system/firmware_
update?attributes=status,failure_reason" \
  -H "accept: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw=="

**Results**
{
  "failure_reason": {
    "description": "Firmware update operation was aborted by user request",
    "number": 3
  },
  "status": "aborted",
```

Use Case 4 - Primary to secondary flash image transfer

1. Start firmware update from the primary to the secondary image location

```
curl -X PATCH "https://1.1.1.2/rest/v10.17/system/firmware_update" \
  -H "accept: */*" \
  -H "Content-Type: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw==" \
  -d '{
    "src_url": "flash:/primary",
    "dst_url": "flash:/secondary",
    "start_request": 105,
  }'
```

2. Monitor status, statistics, and processed_request until the status is either complete or failed

```
curl -X GET "https://1.1.1.2/rest/v10.17/system/firmware_
update?attributes=status,processed_request,statistics" \
  -H "accept: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw=="

**Results**
{
  "processed_request": 105,
  "statistics": {
    "bytes_total": 686059690,
    "bytes_transferred": 686059690,
    "estimated_completion_time": 0,
    "finish_time": 1752787287,
    "percent_complete": 100,
```

```
    "retry_num": 0,
    "start_time": 1752786982,
    "time_elapsed": 305,
    "transfer_rate": 2275936
  },
  "status": "complete"
}
```

Use Case 5 - USB to flash image transfer

1. Start firmware update from a USB flash drive (already inserted and mounted) to the primary image location.

```
curl -X PATCH "https://1.1.1.2/rest/v10.17/system/firmware_update" \
  -H "accept: */*" \
  -H "Content-Type: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw==" \
  -d '{
    "src_url": "usb:/NL_10_17_0001.swi",
    "dst_url": "flash:/primary",
    "start_request": 222,
  }'
```

2. Monitor status, statistics, and processed_request until the status is either complete or failed

```
curl -X GET "https://1.1.1.2/rest/v10.17/system/firmware_
update?attributes=status,processed_request,statistics" \
  -H "accept: application/json" \
  -H "x-csrf-token: MnIMxZb2DHWf6VM8PAgcBw=="

**Results**
{
  "processed_request": 222,
  "statistics": {
    "bytes_total": 686059690,
    "bytes_transferred": 686059690,
    "estimated_completion_time": 0,
    "finish_time": 1752787287,
    "percent_complete": 100,
    "retry_num": 0,
    "start_time": 1752786982,
    "time_elapsed": 305,
    "transfer_rate": 2275936
  },
  "status": "complete"
}
```

Hot-patch software

Overview

Hot-patching provides users of AOS-CX with a way to update running software without rebooting their system. Hot-patches are distributed as signed .patch files and are applied on top of an official AOS-CX image.

A hot-patch can be downloaded from a remote server onto an AOS-CX switch then applied without rebooting the switch. By default, the software patch remains on the switch after it is applied, and is automatically reapplied when the switch reboots. In order to revert an applied hot-patch update, the patch must be disabled. When the hot-patch is disabled, rebooting the box is not necessary, though the hot-patch will still remain on the system. The hot-patch can be removed from the system after disabling the hot-patch.

Once a downloaded hot-patch is removed, it must be downloaded again before it can be reapplied.

Hot-patches are cumulative, meaning that each subsequent patch is a superset of the previous patch(es) for a given software image. When multiple hot-patches are required, the first should be removed after the second has been applied.

Prerequisites

- AOS-CX hot-patch software can be obtained from HPE Aruba Networking customer support, and is identified with a **.patch** extension. The name of the patch indicates the version of AOS-CX to which it can be applied. For example, the patch **FL.10.12.XXXX-YYYY.patch** indicates that the patch can be applied on top of switch image **FL.10.12.XXXX.swi** and brings software up to date with the **FL.10.12.YYYY** release.
- Hot-patch software can be applied only after it has been downloaded to the switch.

Caveats and limitations

- Hot-patch files cannot be managed when the switch is loaded with a .swi image that does not support the hot-patch feature.
- Only restartable daemons can be updated with a hot-patch file.
- Each hot-patch applies to only one release image and each subsequent hot-patch for that release image is cumulative.This means that applying the most recent hot-patch provides all the same fixes included in previous hot-patches. As such, only one hot-patch can be applied at a time.
- incompatible and un-applied hot-patches are allowed to remain on the system and in the config to support rollback to the previous version of the software, and to automatically apply any hot-patches that have been previously applied.
- A maximum of ten hot-patches are allowed to be present or preconfigured on the system at a time.
- A daemon/service may restart if it has a hard dependency on another service that gets restarted by being hot-patched. Upon rebooting, hot-patches are reapplied after daemons have started.
- The **dpsed** and **hpe-cardd** daemon cannot have a hot-patch applied while a switchover or failover is in progress.

To apply a hot-patch update

1. Request a hot-patch from HPE Aruba Networking customer support, then place the hot-patch on an FTP-SFTP server.
2. Use the **copy** command to copy the hot-patch from the remote server to the standalone switch or VSF.
3. Use the **hot-patch apply** command to apply the patch.

To unapply hot-patch update

This option only unapplies the patch, but does not remove the patch from the device. The patch can be reapplied again since it is still on the device. If an unapplied patch needs to be removed/deleted from the switch, it can be removed with the command **hot-patch remove <patch>.patch**.

```
switch(config)# show hot-patch
Name                        Status
-------------------------   ------
FL_10_12_0001-0002.patch    Not applied
switch(config)# hot-patch apply FL_10_12_0001-0002.patch
switch(config)#
switch(config)# show hot-patch
Name                        Status
-------------------------   ------
FL_10_12_0001-0002.patch    Applied

switch(config)# no hot-patch apply FL_10_12_0001-0002.patch
switch(config)# show hot-patch
Name                        Status
-------------------------   ------
FL_10_12_0001-0002.patch    Not applied

switch(config)#
switch(config)# hot-patch remove FL_10_12_0001-0002.patch
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.
switch(config)#
switch(config)# show hot-patch
No hot-patch found or configured
switch(config)#
```

To remove/delete a patch:

An applied hot-patch can be both unapplied and removed from the device with the command **hot-patch remove <patch-name>.patch**. The patch cannot be reapplied unless it is downloaded again.

Checkpoints

A checkpoint is a snapshot of the running configuration of a switch and its relevant metadata during the time of creation. Checkpoints can be used to apply the switch configuration stored within a checkpoint whenever needed, such as to revert to a previous, clean configuration. Checkpoints can be applied to other switches of the same platform. A switch is able to store multiple checkpoints.

Checkpoint types

The switch supports two types of checkpoints:

- **System generated checkpoints**: The switch automatically generates a system checkpoint whenever a configuration change occurs.
- **User generated checkpoints**: The administrator can manually generate a checkpoint whenever required.

Maximum number of checkpoints

- Maximum checkpoints: 64 (including the startup configuration)
- Maximum user checkpoints: 32
- Maximum system checkpoints: 32

User generated checkpoints

User checkpoints can be created at any time, as long as one configuration difference exists since the last checkpoint was created. Checkpoints can be applied to either the running or startup configurations on the switch.

All user generated checkpoints include a time stamp to identify when a checkpoint was created.

A maximum of 32 user generated checkpoints can be created.

System generated checkpoints

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.

Supported remote file formats

You can restore a switch configuration by copying a switch configuration stored on a USB drive or a remote network device through SFTP/TFTP. The remote file formats that the switch supports depends on where you plan to restore the checkpoint.

Restoring a checkpoint to a...	File type supported
Running configuration	▪ CLI ▪ JSON ▪ Checkpoint
Startup configuration	▪ JSON ▪ Checkpoint
Specified checkpoint	Specified checkpoint

Rollback

The term rollback is used to refer to when a switch configuration is reverted to a pre-existing checkpoint.

For example, the following command applies the configuration from checkpoint `ckpt1`. All previous configurations are lost after the execution of this command: `checkpoint rollback ckpt1`

You can also specify the rollback of the running configuration or of the startup configuration with a specified checkpoint, as shown with the following command: `copy checkpoint <checkpoint-name> {running-config | startup-config}`

Checkpoint auto mode

Checkpoint auto mode configures the switch with failover support, causing it to automatically revert to a previous configuration if it becomes inoperable or inaccessible due to configuration changes that are being made.

After entering checkpoint auto mode, you have a set amount of time to add, remove, or modify the existing switch configuration. To save your changes, you must execute the `checkpoint auto confirm` command before the auto mode timer expires. If you do not execute the `checkpoint auto confirm` command within the specified time, all configuration changes you made are discarded and the running configuration reverts to the state it was before entering checkpoint auto mode.

Testing a switch configuration in checkpoint auto mode

Process overview:

1. Enable the checkpoint auto mode.
2. To save the configuration, enter the `checkpoint auto confirm` command before the specified time set in step 1.

Checkpoint commands

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.

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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

checkpoint diff

```
checkpoint diff {<CHECKPOINT-NAME1> | running-config | startup-config}
     {<CHECKPOINT-NAME2> | running-config | startup-config | REMOTE_URL | STORAGE_URL}
[vrf <VRF_NAME>] [deep]
```

Description

Shows the difference in configuration between two configurations. Compare checkpoints, the running configuration, or the startup configuration.

Parameter	Description
{<*CHECKPOINT-NAME1*> | running-config | startup-config}	Selects either a checkpoint, the running configuration, or the startup configuration as the baseline.
{<*CHECKPOINT-NAME2*> | running-config | startup-config}	Selects either a checkpoint, the running configuration, or the startup configuration to compare.
REMOTE_URL | STORAGE-URL	Retrieves a CLI type configuration from a remote or local file. Configurations must be in CLI format.
[vrf <*VRF_NAME*>]	Specifies the VRF name when using a REMOTE_URL to download a checkpoint.
[deep]	Uses a deep mode comparison.

Usage

REMOTE_URL or STORAGE_URL configurations must be in CLI format only, checkpoint format is currently not supported.

In order to get accurate diff results, ensure that the imported file has a valid configuration, correct indentation to represent context changes between CLI contexts, and the file uses the Unix end of line format (\n). The imported file should follow the same syntax and format as the output for **show running-config**. The use of 4 spaces is recommended over the use of tab.

When using the default diff mode, the output of a similar Unix **diff-u** is used. The deep option makes the comparison based on unique entries within a given context instead of based on the order of configuration lines.

The output of the **checkpoint diff** command has several symbols:

- The plus sign (+) at the beginning of a line indicates that the line exists in the comparison but not in the baseline.
- The minus sign (-) at the beginning of a line indicates that the line exists in the baseline but not in the comparison.

- An empty space ( ) is used to represent configuration contexts that exist in both configurations (common) but contain added or removed entries.

Examples

In the following example, the configurations of checkpoints **cp1** and **cp2** are displayed before the `checkpoint diff` command, so that you can see the context of the **checkpoint diff** command.

```
switch# show checkpoint cp1
Checkpoint configuration:
!
!Version AOS-CX XL.10.00.0002
!Schema version 0.1.8
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1,200
interface 1/1/1
    no shutdown
    ip address 1.0.0.1/24
interface 1/1/2
    no shutdown
    ip address 2.0.0.1/24

switch# show checkpoint cp2
Checkpoint configuration:
!
!Version AOS-CX XL.10.00.0002
!Schema version 0.1.8
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1,200,300
interface 1/1/1
    no shutdown
    ip address 1.0.0.1/24
interface 1/1/2
    no shutdown
    ip address 2.0.0.1/24

switch# checkpoint diff cp1 cp2
--- /tmp/chkpt11501550258421    2017-08-01 01:17:38.420514016 +0000
+++ /tmp/chkpt21501550258421    2017-08-01 01:17:38.420514016 +0000
@@ -9,7 +9,7 @@
 !
 !
 !
-vlan 1,200
+vlan 1,200,300
 interface 1/1/1
     no shutdown
     ip address 1.0.0.1/24
```

```
switch# checkpoint diff chkpt01 chkpt02
--- /tmp/chkpt011607564301327
+++ /tmp/chkpt021607564301353
@@ -1,7 +1,7 @@
 !
 !Version AOS-CX PL.10.06.0100V
 !export-password: default
-hostname Switch
+hostname Switch1
 user admin group administrators password ciphertext
AQBapTyg9tpaiAaTfSVV5eNdFzOORRvZ6CMpglh1P+LQUHQLYgAAAGAhmRqFbkNvrgy2SBVk7H8C5hvg/I
ib8rWYFZLEaSCrobNP9EwMu+hLNM0xmsh45yG8dncP7WkxjwrW4p4Qra6dVfr0EW8xh/lpQf8F/2Wki20L
c9JLXiYge7ti0H6cVn+G
 radius-server tracking interval 60
 no usb

switch#
```

Showing the difference in configuration between two configurations using the deep option.

```
switch# checkpoint diff running-config checkpoint run deep
-vlan 1, 100
+vlan 1
```

Showing the difference in configuration between two configurations using the deep option when there are warnings related to the file.

```
switch# checkpoint diff running-config sftp://user@172.17.0.1/config2.txt vrf mgmt
deep(user@172.17.0.1) Password:
sftp> get halon-src/hpe-config/scripts/configdiff/configdiff/config2.txt
userconfig2.txt
-vlan 1, 100
+vlan 1

WARN: Use of tabs is not recommended. File: dest-config2.txt line: 15
WARN: Use of tabs is not recommended. File: dest-config2.txt line: 16
```

Showing the difference in configuration between two configurations using the deep option when there are errors in the file and no diff output is displayed.

```
switch# checkpoint diff running-config sftp://user@172.17.0.1/config.txt vrf  mgmt
 deep(user@172.17.0.1) Password:
sftp> get config.txt userconfig.txt
ERROR: Duplicate entry found. File: dest-config.txt (line 25): 'vlan 2'
```

Command History

Release	Modification
10.16	Updated syntax to include REMOTE_URL, STORAGE_URL, and deep.
10.07 or earlier	--

Command Information

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

checkpoint post-configuration

```
checkpoint post-configuration

no checkpoint post-configuration
```

Description

Enables creation of system generated checkpoints when configuration changes occur. This feature is enabled by default.

The **no** form of this command disables system generated checkpoints.

Usage

System generated checkpoints are automatically created by default. Whenever a configuration change occurs, the switch starts a timeout counter (300 seconds by default). For each additional configuration change, the timeout counter is restarted. If the timeout expires with no additional configuration changes being made, the switch generates a new checkpoint.

System generated checkpoints are named with the prefix **CPC** followed by a time stamp in the format **<YYYYMMDDHHMMSS>**. For example: **CPC20170630073127**.

System checkpoints can be applied using the checkpoint rollback feature or copy command.

A maximum of 32 system checkpoints can be created. Beyond this limit, the newest system checkpoint replaces the oldest system checkpoint.

Examples

Enabling system checkpoints:

```
switch(config)# checkpoint post-configuration
```

Disabling system checkpoints:

```
switch(config)# no checkpoint post-configuration
```

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
```

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.

Parameter	Description
<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
```

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
```

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
```

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
```

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
```

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:
	`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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy *<REMOTE-URL>* startup-config|running-config

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

Description

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

Parameter	Description

<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`

`startup-config`	Indicates that the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration.
`running-config`	Indicates that the running configuration receives the copied checkpoint configuration.
`overwrite`	By default, the CLI configuration contained in the coped file is applied on top of the running-config, so the CLI command does not clear the running-config before applying the CLI commands. In the event that a particular CLI command fails then the failure is logged in event logs and the next line in CLI configuration is processed. When you include the **overwrite** parameter, the configuration is only applied to the running-config if *all* the commands succeeded without errors. If there are any errors during the copy process, the existing running-config will remain intact. You can then inspect the event logs to check and fix the errors and retry the operation. If more than 20 errors are present, the operation stops processing any further commands. The event logs will display only those errors procesed up to that point.
`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
```

Command History

Release	Modification
10.15	The overwrite parameter is introduced.
10.07 or earlier	--

Command Information

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

copy running-config {startup-config | checkpoint <*CHECKPOINT-NAME*>}

`copy running-config {startup-config | checkpoint <CHECKPOINT-NAME>}`

Description

Copies the running configuration to the startup configuration or to a new checkpoint. If the startup configuration is already present, the command overwrites the existing startup configuration.

Parameter	Description
`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. **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
```

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:
	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
```

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
```

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
```

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

Parameter	Description
	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
```

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> |dsm |kernel`	Erase one of the following sets of core-dump files: ■ all: Erase all core-dump files. ■ daemon <daemon-name>: Erase daemon core-dump files. ■ dsm: Erase cord-dump files for the Distributed-services-module. ■ 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
```

Command History

Release	Modification
10.09.0020	The `dsm` 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.

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"
        }
    },
...
...
...
...
```

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.).
```

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
```

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
```

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
```

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>`
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.).
```

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.).
```

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
```

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 commands

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.
```

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#
```

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

Parameter	Description
	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
```

Showing the boot history of the active management module and all line modules:

```
switch#
Management module
=================

Index : 3
Boot ID : f1bf071bdd04492bbf8439c6e479d612
Current Boot, up for 22 hrs 12 mins 22 secs

Index : 2
Boot ID : edfa2d6598d24e989668306c4a56a06d
07 Aug 18 16:28:01 : Reboot requested through database

Index : 1
Boot ID : 0bda8d0361df4a7e8e3acdc1dba5caad
07 Aug 18 14:08:46 : Reboot requested through database

Index : 0
Boot ID : 23da2b0e26d048d7b3f4b6721b69c110
07 Aug 18 13:00:46 : Reboot requested through database

Line module 1/1
=================
```

```
Index : 3
10 Aug 17 12:45:46 : dune_agent crashed
...

Management module
=================

Index : 3
Boot ID : f1bf071bdd04492bbf8439c6e479d612
Current Boot, up for 22 hrs 12 mins 22 secs

Index : 2
Boot ID : edfa2d6598d24e989668306c4a56a06d
07 Aug 18 16:28:01 : Reboot requested through database

Index : 1
Boot ID : 0bda8d0361df4a7e8e3acdc1dba5caad
07 Aug 18 14:08:46 : Reboot requested through database

Index : 0
Boot ID : 23da2b0e26d048d7b3f4b6721b69c110
07 Aug 18 13:00:46 : Reboot requested through database

Line module 1/1
=================
Index : 3
10 Aug 17 12:45:46 : dune_agent crashed
...
```

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.

Firmware management commands

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.

Parameter	Description
	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
```

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
```

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...
```

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:
	`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...
```

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 mgmt
The primary image will be deleted.

Continue (y/n)? y
The authenticity of host '192.22.1.0 (192.22.1.0)' can't be established.
ECDSA key fingerprint is SHA256:MyI1xbdKnehYut0NLfL69gDpNzCmZqBVvBaRR46m7o8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.22.1.0' (ECDSA) to the list of known hosts.
stor@192.22.1.0's password:
Connected to 192.22.1.0.
sftp> get c8d5b9f-topflite.swi c8d5b9f-topflite.swi.dnld
Fetching /home/dr/im-switch.swi to c8d5b9f-topflite.swi.dnld
/home/dr/im-switch.swi                100%  226MB  56.6MB/s   00:04

Verifying and writing system firmware...
```

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...
```

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.

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 HPE Aruba Networking 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.

Command History

Release	Modification
10.12	Hot-patch is now supported on all platforms.
10.10	Command introduced.

Command Information

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

show hot-patch

```
show hot-patch [detail]
```

Parameter	Description
detail	Displays the detailed status of all hot-patches present on the system.

Description

the **show hot-patch** command displays the status of all hot-patches present on the system. The **show hot-patch detail** command displays detailed information for all hot patches present on the system.

Examples

```
switch# show hot-patch

Name                           Status
-----------------------        -------
FL_10_12_0001-0002.patch       Applied

switch# show hot-patch detail

Name                : FL_10_12_0001-0002.patch
Status              : Applied
Version             : FL_10_12_0001-0002.patch
Compatible Version  : FL.10.12.0001
Issues Fixed        : CR1234, CR2345
Patch Date          : 2022-03-29 20:46:15 UTC
Patch ID            : AOS-CX:FL.10.12.0001-sp1-256-gd457e88d39:20220442009
Patch SHA           : a4038d06a2e5fe7e0d457e868d39e526185b
```

Related Commands

Command	Description
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.

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.

gNMI commands

crypto pki application gnmi certificate

```
crypto pki application gnmi certificate <CERT-NAME>
```

Description

Configures a certificate for the gNMI server. **local-cert** is used by default.

Parameter	Description
<CERT-NAME>	Specifies the certificate name.

Examples

Configure sign-cert for the gNMI server:

```
switch(config)# crypto pki application gnmi certificate sign-cert
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 10000	config	Administrators or local user group members with execution rights for this command.

gnmi vrf

```
gnmi vrf <VRF NAME>
no gnmi vrf <VRF NAME>
```

Description

Enables the gNMI server on a given VRF. gNMI can be enabled on multiple VRFs simultaneously.

There is a maximum of 30 gNMI subscriptions per request and a maximum of 9 concurrent streams per switch. These are system-wide limits shared among all authenticated users regardless of connection method (local or remote).

The **no** form of this command removes the configuration.

Disabling the gNMI server on a VRF immediately closes any active streams.

Parameter	Description
<VRF NAME>	Specifies the VRF name.

Examples

Enable the gNMI server on VRF mgmt:

```
switch(config)# gnmi vrf mgmt
```

Removing the configuration of gNMI server on mgmt:

```
switch(config)# no gnmi vrf mgmt
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 10000	config	Administrators or local user group members with execution rights for this command.

show gnmi

```
show gnmi
```

Description

Displays the current gNMI configuration.

Examples

Display the current gNMI configuration:

```
switch(config)# show gmni
gNMI Configuration
------------------------------------------------------------
VRF                  : mgmt, default
Access mode          : read-only
Global stream limit  : 9
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8360 9300 10000	`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.

Chapter 11
Dynamic Segmentation

For information on dynamic segmentation, view the *Security Guide*.

Chapter 12
SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing and monitoring the devices connected to a network by collecting, organizing and modifying information about managed devices on IP networks.

Configuring SNMP

(The SNMP agent provides read-only access.)

Procedure

1. Enable SNMP on a VRF using the command `snmp-server vrf`.
2. Set the system contact, location, and description for the switch with the following commands:
   - `snmp-server system-contact`
   - `snmp-server system-location`
   - `snmp-server system-description`
3. If required, change the default SNMP port on which the agent listens for requests with the command `snmp-server agent-port`.
4. By default, the agent uses the community string **public** to protect access through SNMPv1/v2c. Set a new community string with the command `snmp-server community`.
5. Configure the trap receivers to which the SNMP agent will send trap notifications with the command `snmp-server host`.
6. Create an SNMPv3 context and associate it with any available SNMPv3 user to perform context specific v3 MIB polling using the command `snmpv3 user` .
7. Create an SNMPv3 context and associate it with an available SNMPv1/v2c community string to perform context specific v1/v2c MIB polling using the command `snmpv3 context`.
8. Review your SNMP configuration settings with the following commands:
   - `show snmp agent-port`
   - `show snmp community`
   - `show snmp system`
   - `show snmpv3 context`
   - `show snmp trap`
   - `show snmp vrf`
   - `show snmpv3 users`
   - `show tech snmp`

Example 1

This example creates the following configuration:

- Enables SNMP on the out-of-band management interface (VRF **mgmt**).
- Sets the contact, location, and description for the switch to: **JaniceM**, **Building2**, **LabSwitch**.
- Sets the community string to **Lab8899X**.

```
switch(config)# snmp-server vrf mgmt
switch(config)# snmp-server system-contact JaniceM
switch(config)# snmp-server system-location Building2
switch(config)# snmp-server system-description LabSwitch
switch(config)# snmp-server community Lab8899X
```

Example 2

This example creates the following configuration:

- Creates an SNMPv3 user named **Admin** using **sha** authentication with the plaintext password **mypassword** and using **des** security with the plaintext password **myprivpass**.
- Associates the SNMPv3 user `Admin` with a context named `newContext`.

```
switch(config)# snmpv3 user Admin auth sha auth-pass plaintext mypassword priv des
     priv-pass plaintext myprivpass
switch(config)# snmpv3 user Admin context newContext
```

Refer to the SNMP Guide for SNMP Commands.

Chapter 13

HPE Aruba Networking Central

The HPE Aruba Networking Central network management solution, a software-as-a-service subscription in the cloud, provides streamlined management of multiple network devices. AOS-CX switches are able to talk to HPE Aruba Networking Central and utilize cloud-based management functionality. Cloud-based management functionality allows for the deployment of network devices at sites with no or few dedicated IT personnel (branch offices, retail stores, and so forth). AOS-CX switches utilize secure communication protocols to connect to the HPE Aruba Networking Central cloud portal, and can coexist with corporate security standards, such as those mandating the use of firewalls.

When HPE Aruba Networking Central manages AOS-CX switches, it functions as the single source of truth and the Web UI operates in read-only mode.

This feature provides:

- Zero-touch provisioning
- Network Management/Remote monitoring
- Events/alerts notification
- Switch Configuration using templates
- Firmware management

Connecting to HPE Aruba NetworkingCentral

AOS-CX switch downloads the location of HPE Aruba Networking Central server using:

- Command-line interface (CLI).
- HPE GreenLake server.
- DHCP options provided during ZTP.

DHCP servers are used to connect to Central on-premise management.

When a switch is able to connect to HPE Aruba Networking Central, but is not registered in the HPE Aruba Networking Central inventory or does not have a proper license, the switch will get disconnected. If the HPE Aruba Networking Central feature is enabled using this command, the switch will then reconnect back to HPE Aruba Networking Central and will get disconnected again. This connect/disconnect process will continue until the switch is properly registered in HPE Aruba Networking Central. To avoid this unnecessary reconnection cycle, best practices is to disable HPE Aruba Networking Central until the switch is registered in HPE Aruba Networking Central, or a license is obtained for that device.

Custom CA certificate

To use a custom CA certificate to connect to HPE Aruba Networking Central, AOS-CX switch downloads the certificate from the HPE GreenLake server.

- If there is no custom CA provided by HPE GreenLake, the CA certificate present in the device is used.
- Duplicate CA certificates from HPE GreenLake server will be ignored.
- If CA certificate is absent in consecutive responses from the HPE GreenLake server, the installed custom CA certificate in device will be removed.
- Switch will have only one custom CA certificate installed from the HPE GreenLake Server.
- The certificate installed from the HPE GreenLake server will not be displayed in the show commands.

Support mode in HPE Aruba Networking Central

When the AOS-CX switch is managed by HPE Aruba Networking Central, the switch configuration cannot be modified using other interfaces such as CLI or Web UI. The following command categories are blocked:

- auto-confirm
- boot
- checkpoint
- copy-in commands
- erase
- erps
- https-server
- mfgread
- mfgwrite
- port-access
- All configuration commands except the aruba-central command

In cases where a maintenance or troubleshooting activity requires configuration updates, aruba-central support-mode can be enabled to allow these operations.

The aruba-central support-mode enable or disable operation is effective only in the CLI session where it is executed and does not impact the other CLI sessions.

If the user tries to execute any command that is not allowed, an **Invalid input:** error message is displayed.

One Touch Provisioning

One Touch Provisioning (OTP) allows a switch to be provisioned on HPE Aruba Networking Central with the minimum user configuration.

Configuring One Touch Provisioning

To provision a switch to HPE Aruba Networking Central by using an OTP scenario, you can configure:

- The HPE Aruba Networking Central Location

Following configurations can be done optionally:

- The Domain Name System (DNS) server address.
- The HTTP proxy location.

Configuring HPE Aruba Networking Central location

1. Create the hpe-anw-central context.

```
switch(config)# hpe-anw-central
```

2. Configure the HPE Aruba Networking Central server location

```
switch(hpe-anw-central)# location-override <LOCATION> vrf <VRF>
```

IPv4 or IPv6 address can be used.

3. Validate the connectivity status to HPE Aruba Networking Central

```
switch# show hpe-anw-central
```

Configuring DNS server address

1. Configure the DNS server address.

```
switch(config)# ip dns server-address <ADDRESS> vrf <VRF>
```

IPv4 or IPv6 a ddress can be used.

2. Validate the DNS server status

```
switch# show ip dns
```

Configuring HTTP proxy location

1. Configure the HTTP Proxy location

```
switch(config)# http-proxy <LOCATION> vrf <VRF>
```

LOCATION can be either a FQDN, IPv4 address or IPv6 address

Limitations for Zero Touch Provisioning

The following are the limitations for OTP when provisioning a switch by using IPv6:

- Support for obtaning the HPE Aruba Networking Central location via DHCP.
- Support for connectivity to an HPE Aruba Networking Central on-premise instance.

Supportability

Debug logging can be enabled with the following command:

The central debug logs are helpful to determine connectivity issues with HPE Aruba Networking Central.

```
switch# debug central all
```

HPE Aruba Networking Central commands

hpe-anw-central

```
hpe-anw-central
no hpe-anw-central
```

Description

Creates or enters the HPE Aruba Networking Central configuration context (**config-hpe-anw-central**).

When a switch is able to connect to HPE Aruba Networking Central but is not registered in the HPE Aruba Networking Central inventory or does not have a proper license, the switch will get disconnected. If the HPE Aruba Networking Central feature is enabled using this command, the switch will then reconnect back to HPE Aruba Networking Central and will get disconnected again. This connect/disconnect process will continue until the switch is properly registered in HPE Aruba Networking Central. To avoid this unnecessary reconnection cycle, best practices is to disable HPE Aruba Networking Central until the switch is registered in HPE Aruba Networking Central, or a license is obtained for that device.

Example

Creating the HPE Aruba Networking Central configuration context:

```
switch(config)# hpe-anw-central
switch(config-hpe-anw-central)#
```

Command History

Release	Modification
10.15	Command syntax changed from **aruba-central** to **hpe-anw-central.**
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config	Administrators or local user group members with execution rights for this command.

hpe-anw-central support-mode

```
hpe-anw-central support-mode
no hpe-anw-central support-mode
```

Description

Allows the device to be writable for all operations in HPE Aruba Networking Central lockout mode for troubleshooting. The no form of this command disables this activity.

Support-mode is disabled by default when the switch is managed by HPE Aruba Networking Central. This command is only effective in the CLI session where it is executed.

Examples

Configuring the device to be writable for all operations in HPE Aruba Networking Central lockout mode:

```
switch# hpe-anw-central support-mode
```

Removing the configuration that allows the device to be writable for all operations in HPE Aruba Networking Central lockout mode:

```
switch# no hpe-anw-central support-mode
switch#
```

Command History

Release	Modification
10.15	Command syntax changed from **aruba-central** to **hpe-anw-central.**
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320	Manager (#)	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8325 8325H 8325P 8360 9300 9300S 10000		

configuration-lockout central managed

```
configuration-lockout central managed
no configuration-lockout central managed
```

Description

Configures the device to only be writable from HPE Aruba Networking Central. HPE Aruba Networking Central will be the only agent that can add, modify, or delete configurations on the device. The no form of this command disables this feature.

The no form of this command is only available when the device is disconnected from HPE Aruba Networking Central.

Usage

The AOS-CX switch connects to HPE Aruba Networking Central in either of two modes: monitor or managed. When the device is connected in monitor mode, HPE Aruba Networking Central monitors the configurations on the switch. When the device is connected in managed mode, the **configuration-lockout central managed** command does not allow configuration changes from other interfaces such as CLI or Web UI.

Examples

Configuring the device to only be writable from HPE Aruba Networking Central :

```
switch(config)# configuration-lockout central managed
switch# show configuration-lockout
configuration lockout
---------------------
central: managed
switch# sh hpe-anw-central
Central admin state                  :enable
Central location                     :20.0.0.2:8083
VRF for connection                   :default
Central connection status            :connected

Central source                       :cli
Central source connection status     :connected
Central source last connected on     :Tue Feb 9 17:53:13 UTC 2021

Activate Server URL                  :devices-v2.arubanetworks.com
CLI location                         :20.0.2:8083
CLI VRF                              :default
switch(config)# end
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	`config`	Administrators or local user group members with execution rights for this command.

diag-dump rest basic

`diag-dump rest basic`

Description

Display REST paths and diagnostics information for the REST feature. The output of this command includes diagnostics information for HPE Aruba Networking Central.

Example

The following example displays just the **Central Counters** portion of the output for this command.

```
switch# diag-dump rest basic
================================================================================
[Start] Feature rest Time : Sun Sep 17 17:06:50 2023
================================================================================
...
...
...
Central Counters:
----------------------------------------
Logins:                                 1
Connections:                            1
Disconnections:                         0
----------------------------------------
Pings:                                  50
Pongs:                                  50
----------------------------------------
API Requests:                           20
Response API Requests:                  20
----------------------------------------
v1 Notification Requests Received:      5
v1 Notifications Sent:                  15
Initial Snapshots:                      5
Notifications:                          10
Errors:                                 0
----------------------------------------
v2 Notification Requests Received:      10
v2 Notifications Sent:                  24
Initial Snapshots:                      10
```

```
Unsubscribes:                         0
Notifications:                        14
Errors:                               0
---------------------------------------
Views Notification Requests:          0
Views Notification Responses:         0
Views Unary Requests:                 0
Views Unary Responses:                0
---------------------------------------
Packet Capture Responses:             0
---------------------------------------
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

disable

`disable`

Description

Disables connection to HPE Aruba Networking Central server.

When the connection is disabled, the switch does not attempt to connect to the HPE Aruba Networking Central server or fetch central location from any of the three sources (CLI/HPE GreenLake/DHCP). It also disconnects any active connection to the HPE Aruba Networking Central server.

Example

```
switch(config-hpe-anw-central)# disable
switch(config-hpe-anw-central)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320	`config-hpe_anw-central`	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8325 8325H 8325P 8360 9300 9300S 10000		

enable

`enable`

Description

Enables connection to HPE Aruba Networking Central server. When the connection is enabled, the switch attempts to download the location of the HPE Aruba Networking Central server in one of the following ways at startup and after the connection is lost:

- Using command-line interface (CLI).
- Connecting to the HPE GreenLake server.
- Using DHCP options provided during ZTP.

DHCP servers provide the options requested by the device to connect to Central, Central On-premise managment, or the TFTP server.

When a switch is able to connect to HPE Aruba Networking Central, but is not registered in the HPE Aruba Networking Central inventory or does not have a proper license, the switch will get disconnected. If the HPE Aruba Networking Central feature is enabled using this command, the switch will then reconnect back to HPE Aruba Networking Central and will get disconnected again. This connect/disconnect process will continue until the switch is properly registered in HPE Aruba Networking Central. To avoid this unnecessary reconnection cycle, best practices is to disable HPE Aruba Networking Central until the switch is registered in HPE Aruba Networking Central, or a license is obtained for that device.

Examples

```
switch(config-hpe-anw-central)# enable
switch(config-hpe-anw-central)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320	`config-hpe_anw-central`	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
8325 8325H 8325P 8360 9300 9300S 10000		

location-override

```
location-override <location> [vrf <VRF-NAME>]
no location-override
```

Description

When **location** and **vrf** are configured, the switch overrides existing connections to HPE Aruba Networking Central. The switch attempts to establish connection to HPE Aruba Networking Central with the specified location and VRF with highest priority.

Location can take one of the following values:

- A fully qualified domain name (FQDN) along with an optional port number.
- An IPv4 address with an optional port number.
- An IPv6 address with an optional port number.

If the port number is not specified, then port 443 is used by default. If the command is executed without the VRF parameter, the switch uses

the 'default' VRF.

The **no** form of this command removes location override values from the HPE Aruba Networking Central configuration context.

When you configure an IPv6 address with a port number, specify the address part inside square brackets, optionally followed by the port number, e.g. [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443.

Parameter	Description
<location>	Specifies one of these values: ■ *<FQDN>*: a fully qualified domain name. ■ *<IPV4>*: an IPv4 address. ■ *<IPV6>*: an IPv6 address.
`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

Configuring location override with location and VRF:

```
switch(config-hpe-anw-central)# location-override hpe-anw-central.com vrf default
switch(config-hpe-anw-central)#
```

```
switch(config-hpe-anw-central)# location-override hpe-anw-central.com vrf red
switch(config-hpe-anw-central)# location-override 10.0.0.1 vrf red
switch(config-hpe-anw-central)# location-override 10.0.0.1:443 vrf red
switch(config-hpe-anw-central)# location-override
2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf red
switch(config-hpe-anw-central)# location-override
[2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443 vrf red
```

Configuring location override with location only:

```
switch(config-hpe-anw-central)# location-override hpe-anw-central.com
switch(config-hpe-anw-central)#
```

Removing location override values from the HPE Aruba Networking Central configuration context:

```
switch(config-hpe-anw-central)# no location-override
switch(config-hpe-anw-central)#
```

Command History

Release	Modification
10.13.1000	Command updated to reflect an OTP scenario.
10.07 or earlier	--

Command Information

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

location-override-alternative

```
location-override-alternative <LOCATION> [vrf <VRF>]
no location-override-alternative <LOCATION> [vrf <VRF>]
```

Description

Configures information about HPE Aruba Networking Central connection when the alternative location is used.

The **no** form of this command removes the **location-override-alternative** configuration.

Parameter	Description
<LOCATION>	Specifies the HPE Aruba Networking Central location.
`vrf <VRF>`	Specifies the VRF used to connect to HPE Aruba Networking Central.

Usage

When the main and alternative HPE Aruba Networking Central server locations are specified, the switch attempts to connect to the main HPE Aruba Networking Central server. If there is connectivity failure with the main HPE Aruba Networking Central server location, it attempts to establish a connection with the alternative server location.

If the alternative location is configured without a main location, the user is prompted for confirmation. In this case, there is no redundancy and the switch attempts to connect to the alternative location.

Location can take one of the following values:

- A fully qualified domain name (FQDN) along with an optional port number.
- An IPv4 address with an optional port number.
- An IPv6 address with an optional port number.

If the port number is not specified, then port 443 is used by default. If the command is executed without the VRF parameter, the switch uses

the 'default' VRF.

An HPE Aruba Networking Central server location can only be a fully qualified domain name (FQDN) or a valid IP address. If the command is entered without the VRF parameter, the switch uses the default VRF.

Examples

Example of configuring with the hpe-anw-central.com location and VRF red:

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

Example of a configuration with location only:

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

Example of removing the override configuration:

```
switch(config-hpe-anw-central)# no location-override-alternative
switch(config-hpe-anw-central)# location-override-alternative 10.0.0.1 vrf red
switch(config-hpe-anw-central)# location-override-alternative 10.0.0.1:443 vrf red
switch(config-hpe-anw-central)# location-override-alternative
2001:0db8:85a3:0000:0000:8a2e:0370:7334 vrf red
switch(config-hpe-anw-central)# location-override-alternative
[2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443 vrf red
```

Command History

Release	Modification
10.13.1000	Command updated to reflect OTP scenario.
10.12.1000	Command introduced.

Command Information

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

show hpe-anw-central

```
show hpe-anw-central
```

Description

Shows information about HPE Aruba Networking Central connection and the status of the Activate server connection.

Examples

Example of a switch that has the HPE Aruba Networking Central connection:

```
switch# show hpe-anw-central
Central admin state                      : enabled
Central location                         : 10.0.0.1
VRF for connection                       : mgmt
Shared Token                             : N/A
Central connection status                : connected
Central source                           : activate
Central source connection status         : connected
Central source last connected on         : Wed Jun 28 23:07:25 UTC 2023
Main location                            : 10.0.0.1
Main VRF                                 : mgmt
Alternative location                     : N/A
Alternative VRF                          : N/A
Activate Server URL                      : devices-v2.arubanetworks.com
System time synchronized from Activate   : N/A
Source IP                                : N/A
Source IP Overridden                     : False
Central support mode                     : disabled
```

Example of a switch when the main CLI location is used:

```
switch# show hpe-anw-central
Central admin state                     : enabled
Central location                        : 10.0.0.1
VRF for connection                      : mgmt
Shared secret                           : N/A
Central connection status               : connected
Central source                          : cli
Central source connection status        : connected
Central source last connected on        : Wed Jun 28 23:07:25 UTC 2023
Main location                           : 10.0.0.1
Main VRF                                : mgmt
Alternative location                    : 20.0.0.1
Alternative VRF                         : N/A
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                               : N/A
Source IP Overridden                    : False
Central support mode                    : disabled
```

Example of a switch when the alternative CLI location is used:

```
switch# show hpe-anw-central
Central admin state                     : enabled
Central location                        : 20.0.0.1
VRF for connection                      : default
Shared secret                           : N/A
Central connection status               : connected
Central source                          : cli
Central source connection status        : connected
Central source last connected on        : Wed Jun 28 23:07:25 UTC 2023
Main location                           : 10.0.0.1
Main VRF                                : mgmt
Alternative location                    : 20.0.0.1
Alternative VRF                         : default
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate  : N/A
Source IP                               : N/A
Source IP Overridden                    : False
Central support mode                    : disabled
Central admin state                     : enabled
Central location                        : 20.0.0.1
VRF for connection                      : default
Shared secret                           : N/A
Central connection status               : connected
Central source                          : cli
Central source connection status        : connected
Central source last connected on        : Wed Jun 28 23:07:25 UTC 2023
Main location                           : 10.0.0.1
Main VRF                                : mgmt
Alternative location                    : 20.0.0.1
Alternative VRF                         : N/A
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate  : N/A
Source IP                               : N/A
Source IP Overridden                    : False
Central support mode                    : disabled
```

Example of a switch when the location is obtained from DHCP options:

```
switch# show hpe-anw-central
Central admin state                     : enabled
Central location                        : central-western-us.arubanetworks.com
VRF for connection                      : mgmt
Shared secret                           : N/A
Central connection status               : connected
Central source                          : DHCP
Central source connection status        : connected
Central source last connected on        : Fri Jun 30 20:22:33 UTC 2023
Main location                           : central-western-us.arubanetworks.com
Main VRF                                : mgmt
Alternative location                    : N/A
Alternative VRF                         : N/A
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate  : N/A
Source IP                               : 100.0.0.1
Source IP Overridden                    : False
Central support mode                    : disabled
```

Example of a switch when HPE Aruba Networking Central is disabled:

```
switch# show hpe-anw-central
Central admin state                     : disabled
Central location                        : N/A
VRF for connection                      : N/A
Shared secret                           : N/A
Central connection status               : N/A
Central source                          : none
Central source connection status        : N/A
Central source last connected on        : N/A
Main location                           : N/A
Main VRF                                : N/A
Alternative location                    : N/A
Alternative VRF                         : N/A
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                               : N/A
Source IP Overridden                    : False
Central support mode                    : disabled
Central admin state                     : disabled
Central location                        : N/A
VRF for connection                      : N/A
Shared secret                           : N/A
Central connection status               : N/A
Central source                          : none
Central source connection status        : N/A
Central source last connected on        : N/A
Main location                           : N/A
Main VRF                                : N/A
Alternative location                    : N/A
Alternative VRF                         : N/A
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                               : N/A
Source IP Overridden                    : False
Central support mode                    : disabled
```

Example of a switch when HPE Aruba Networking Central is not reachable:

```
switch# show hpe-anw-central
Central admin state                     : enabled
Central location                        : N/A
VRF for connection                      : N/A
Shared secret                           : N/A
Central connection status               : not-reachable
Central source                          : activate
Central source connection status        : connected
Central source last connected on        : Fri Jun 30 20:22:33 UTC 2023
Main location                           : N/A
Main VRF                                : N/A
Alternative location                    : N/A
Alternative VRF                         : N/A
Activate server URL                     : devices-v2.arubanetworks.com
System time synchronized from Activate : N/A
Source IP                               : N/A
Source IP Overridden                    : False
Central support mode                    : disabled
```

Command History

Release	Modification
10.15	Command syntax changed from **aruba-central** to **hpe-anw-central.**
10.12.1000	Enhanced to support more scenarios
10.07 or earlier	--

Command Information

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

show running-config current-context

```
show running-config current-context
```

Description

Shows the running configuration for the current-context. If user is in the context of HPE Aruba Networking Central (**config-hpe-anw-central**), then the HPE Aruba Networking Central running configuration is displayed.

Examples

Shows the running configuration of HPE Aruba Networking Central:

```
switch(config-hpe-anw-central)# show running-config current-context
hpe-anw-central
       disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Troubleshooting

Prerequisites

Enable **support-mode**

Execute the following command to enable support mode on the switch. This allows the execution of CLI commands when Central is the source of truth. This way, the user can use the start-shell command to start a bash shell to run additional debugging commands:

```
switch# hpe-anw-central support-mode
```

Next, disable support mode:

```
switch# no hpe-anw-central support-mode
```

Troubleshooting Scenarios

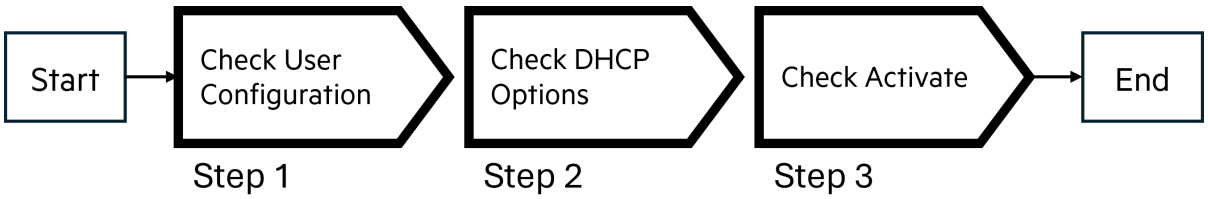
Scenario: Central location discovery

The CX switch cannot obtain the Central location to establish connectivity. The switch attempts to retrieve the Central location from one of the following sources in priority order:

1. User configuration (via CLI or REST API)
2. DHCP options (from DHCP server)
3. Activate server

If the Central location cannot be acquired from any of these sources, connectivity to Central cannot be established. The switch retries these sources using an exponential backoff with the following sequence: 0s, 2s, 4s, 8s, 16s, 32s, 64s.

Troubleshooting Workflow Diagram



Troubleshooting Workflow Steps

Step 1: Verify user configuration

If the Central location is configured via CLI or REST API, verify the configuration.

Diagnostic Command 1.1: Check location and location alternative override.

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central location_override_location location_override_
location_alternative -flist

HPE_ANW_Central table

location_override_location: "test.central.com"
location_override_location_alternative: "test2.central.com"
```

Evaluation: Verify the values match the user configuration. The location alternative may be empty if not configured.

Diagnostic Command 1.2: Check VRF and VRF alternative override.

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central location_override_vrf location_override_vrf_
alternative -flist

HPE_ANW_Central table

location_override_vrf: 9b99f005-5051-473e-a13e-029b576e9776
location_override_vrf_alternative: 9b99f005-5051-473e-a13e-029b576e9776
```

Evaluation: The output contains UUIDs. Match them with VRF names using:

```
switch# start-shell
ovsdb-client dump VRF name _uuid

VRF table_uuid                       name
------------------------------------ -------------------------------------
619e1c63-94a3-44dc-8728-3b831e77bb55 default
9b99f005-5051-473e-a13e-029b576e9776 mgmt
HPE_ANW_Central table
```

Verify the VRF values match the user configuration. The VRF alternative may be empty if not configured.

Diagnostic Command 1.3: Check central source value.

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central central_source central_source_alternative -flist

HPE_ANW_Central table

central_source: cli
central_source_alternative: cli
```

Evaluation: The **central_source** value must be set to **cli**. The central source alternative may be empty if not configured.

Diagnostic Command 1.4: Check final location and VRF

```
switch# start-shell
```

```
ovsdb-client dump HPE_ANW_Central location location_alternative vrf vrf_
alternative -flist

HPE_ANW_Central table

location: "test.central.com"
location_alternative: "test2.central.com"
vrf: 9b99f005-5051-473e-a13e-029b576e9776
vrf_alternative: 9b99f005-5051-473e-a13e-029b576e9776
```

Evaluation: These are the final location and VRF values used to connect to Central. Verify they match the user configuration. The location alternative and VRF alternative may be empty if not configured.

Corrective Action: If values do not match the expected configuration, reconfigure Central location using the appropriate CLI commands or REST requests.

Step 2: Verify DHCP options

If user configuration is not set, the switch retrieves the Central location from DHCP options via a DHCP server.

Diagnostic Command 2.1: Check operational DHCP options

```
switch# start-shell
ovsdb-client dump System operational_dhcp_options

System table
operational_dhcp_options
------------------------------------------------------------------------------
------------------------------------------------------------------------
{central_location="test.central.com", central_location_source=dhcp-vlan1, central_
location_vrf_name=default, central_location_alternative="test2.central.com",
central_location_alternative_source=dhcp-vlan1, central_location_alternative_vrf_
name=default}
```

Evaluation:

- Verify **central_location** and **central_location_alternative** match the DHCP server configuration. The location alternative may be empty if not configured.
- Verify **central_location_source** is set to either **dhcp-mgmt** or **dhcp-vlan**.
- Verify **central_location_vrf_name** matches the VRF through which the DHCP server is accessible.

Diagnostic Command 2.2: Check central source value

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central central_source central_source_alternative -flist

HPE_ANW_Central table

central_source: dhcp
central_source_alternative: dhcp
```

Evaluation: The central_source value must be set to dhcp. The central source alternative may be empty if not configured.

Diagnostic Command 2.3: Check final location and VRF

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central location location_alternative vrf vrf_
alternative -flist

HPE_ANW_Central table

location: "test.central.com"
location_alternative: "test2.central.com"
vrf: 619e1c63-94a3-44dc-8728-3b831e77bb55
vrf_alternative: 619e1c63-94a3-44dc-8728-3b831e77bb55
```

Evaluation: These are the final location and VRF values used to connect to Central. Verify they match the DHCP server configuration. The location alternative and VRF alternative may be empty if not configured.

Corrective Action: If values do not match, verify the DHCP server configuration includes the correct Central location options and that the switch can reach the DHCP server.

Step 3: Verify Activate configuration

If neither user configuration nor DHCP options are available, the switch attempts to retrieve the Central location from the Activate server.

Diagnostic Command 3.1: Check central source value

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central central_source -flist

HPE_ANW_Central table

central_source: activate
```

Evaluation: The central_source value must be set to activate.

Diagnostic Command 3.2: Check final location and VRF

```
switch# start-shell
ovsdb-client dump HPE_ANW_Central location vrf -flist

HPE_ANW_Central table

location: "test.central.com"
vrf: 619e1c63-94a3-44dc-8728-3b831e77bb55
```

Evaluation: These are the final location and VRF values used to connect to Central. Verify they match the Activate server configuration.

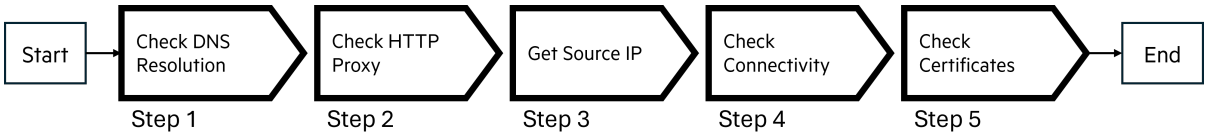
Corrective Action: If values are incorrect, verify the Activate server configuration and ensure the switch can reach the Activate server.

Scenario: Central connectivity

The CX switch cannot establish or maintain connectivity with Central. This can occur with both Cloud-based Central and Central on Premise (COP) deployments. Connectivity issues may manifest as:

- Failed initial connection attempts
- Intermittent disconnections
- Connection timeouts
- Certificate validation errors

Troubleshooting Workflow Diagram



Troubleshooting Workflow Steps

Step 1: Verify DNS resolution

If the Central location uses a fully qualified domain name (FQDN), verify that the switch can resolve the name.

Diagnostic Command:

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
nslookup <Central URL>
```

Example:

```
switch# start-shell
sudo start_vrf_shell default
nslookup test.central.com
```

Evaluation: Verify the DNS query returns a valid IP address.

Corrective Action: If DNS resolution fails:

- Verify the Central URL is correct.
- Verify the DNS server configuration on the switch.
- Ensure the switch can reach the configured DNS server.

Step 2: Verify HTTP proxy configuration

If an HTTP proxy server is configured on the same VRF used for Central connectivity, verify connectivity to the proxy server.

Diagnostic Command 2.1: Check for HTTP proxy configuration

```
switch# start-shell
ovsdb-client dump System operational_dhcp_options

System table
operational_dhcp_options
```

```
------------------------------------------------------------------------------
--------------------------------------
{http_proxy_location="198.51.100.33:8080", http_proxy_location_source=user-
configured, http_proxy_location_vrf_name=default}
```

Evaluation: If http_proxy_location and http_proxy_location_vrf_name are present and the VRF matches the Central VRF, proxy connectivity must be verified.

Diagnostic Command 2.2: Test proxy connectivity

```
switch# start-shell
sudo start_vrf_shell <Proxy VRF>
curl -v http://<Proxy URL>
```

Example:

```
switch# start-shell
sudo start_vrf_shell default
curl -v http://198.51.100.33:8080
*   Trying 198.51.100.33:8080...
* Connected to 198.51.100.33 (198.51.100.33) port 8080
> GET / HTTP/1.1
> Host: 198.51.100.33:8080
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
```

Evaluation: Verify a successful connection is established.

Corrective Action: If proxy connection fails, verify proxy server configuration and network connectivity.

Step 3: Determine source IP configuration

Verify if a source IP is configured for Central connectivity.

Diagnostic Command:

```
switch# start-shell
ovsdb-client dump VRF name effective_source_ip

VRF table
effective_source_ip                          name
-------------------------------------------- ----------------------------------
-----------
{}                                           mgmt
{all="192.0.2.1", central="192.0.2.1"}       default
```

Evaluation:

- If the central key is present, it specifies the source IP for Central traffic.
- If only the all key is present, it provides the source IP for all outgoing packets, including Central traffic.
- If neither is present, routing rules determine the source IP.

Step 4: Verify network MTU support

Test that the configured MTU is supported by the network path to Central.

Diagnostic Command:

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
ping -M do -s <MTU to check> <Central URL>
```

Example: To test an MTU of 1500, subtract 28 from the value: 1500 - 28 = 1472

```
switch# start-shell
sudo start_vrf_shell default
ping -M do -s 1472 test.central.com
```

Evaluation:

- If the command hangs without error messages, the MTU is supported.
- If message too long errors appear, the MTU is too large or a device in the path has a smaller MTU.

Corrective Action: If MTU issues are detected:

- Verify MTU settings on the switch.
- Verify MTU settings on intermediate network devices.

Step 5: Test basic connectivity to Central

Verify that the switch can establish an HTTPS connection to Central.

Diagnostic Command:

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
curl -I -k -v [-x <Proxy URL>] [--interface <Source IP>] \
https://<Central URL>/wss
```

Example:

```
switch# start-shell
sudo start_vrf_shell default
curl -I -k -v -x 198.51.100.33:8080 --interface 192.0.2.1 \
https://test.central.com/wss

* Trying 198.51.100.33:8080...
* Name '192.0.2.1' family 2 resolved to '192.0.2.1' family 2
* Local port: 0
* Connected to 198.51.100.33 (198.51.100.33) port 443
* CONNECT tunnel: HTTP/1.1 negotiated
```

```
* allocate connect buffer
* Establish HTTP proxy tunnel to test.central.com:443
> CONNECT test.central.com:443 HTTP/1.1
> Host: test.central.com:443
> User-Agent: curl/8.7.1
> Proxy-Connection: Keep-Alive
>
< HTTP/1.1 200 Connection Established
HTTP/1.1 200 Connection Established
< Proxy-Agent: Squid/7.1
Proxy-Agent: Squid/7.1
<
* CONNECT phase completed
* CONNECT tunnel established, response 200
* ALPN: curl offers http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256 / x25519 / RSASSA-PSS
* ALPN: server accepted http/1.1
* Server certificate:
*  subject: C=US; ST=California; L=Santa Clara; O=Hewlett Packard Enterprise
Development; OU=Aruba; CN=test.central.com
*  start date: May  7 09:19:17 2025 GMT
*  expire date: May  6 10:19:17 2026 GMT
*  issuer: CN=Test PKI - HPE Aruba Cloud - Aruba Central CA 412; OU=Aruba;
O=Hewlett Packard Enterprise Development; L=Santa Clara; ST=California; C=US
*  SSL certificate verify result: self-signed certificate in certificate chain
(19), continuing anyway.
*   Certificate level 0: Public key type RSA (2048/112 Bits/secBits), signed using
sha256WithRSAEncryption
*   Certificate level 1: Public key type RSA (4096/152 Bits/secBits), signed using
sha256WithRSAEncryption
*   Certificate level 2: Public key type RSA (2048/112 Bits/secBits), signed using
sha256WithRSAEncryption
*   Certificate level 3: Public key type RSA (2048/112 Bits/secBits), signed using
sha256WithRSAEncryption
* using HTTP/1.x
> HEAD /wss HTTP/1.1
> Host: test.central.com
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 502 Bad Gateway
HTTP/1.1 502 Bad Gateway
< Date: Tue, 26 Aug 2025 14:46:27 GMT
Date: Tue, 26 Aug 2025 14:46:27 GMT
< Content-Type: text/html
Content-Type: text/html
< Content-Length: 150
Content-Length: 150
< Connection: keep-alive
Connection: keep-alive
```

```
< Strict-Transport-Security: max-age=3600; includeSubDomains
Strict-Transport-Security: max-age=3600; includeSubDomains
< X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
< X-Request-Start: t=1756219587.032
X-Request-Start: t=1756219587.032
< X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
< allow-cross-namespace-resources: true
allow-cross-namespace-resources: true
< allow-snippet-annotations: true
allow-snippet-annotations: true
< annotations-risk-level: Critical
annotations-risk-level: Critical
<
* Connection #0 to host 198.51.100.33 left intact
```

Evaluation: Receiving any HTTP response code (commonly 502 Bad Gateway) confirms basic connectivity. This response is expected as no information is being sent to the server, but receiving any HTTP code confirms that the connection to the server can be established.

Include the -x <Proxy URL> flag only if an HTTP proxy is configured. Include the --interface <Source IP> flag only if a source IP is configured.

Corrective Action: If no response is received:

- Verify network connectivity between the switch and Central.
- Check firewall rules that may block HTTPS traffic.
- Verify the Central URL is correct and accessible.

Step 6: Verify device and server certificates

Ensure the switch has a valid device certificate and can validate the Central server certificate.

Diagnostic Command 6.1: Verify device certificate

```
switch# show crypto pki certificate

Certificate Name                Cert Status                     EST Status
 Associated Applications
------------------------------- ------------------------------- ----------------
- ------------------------------
device-identity                 installed                       n/a
 none
```

Evaluation: Verify the device-identity certificate is present and installed.

Diagnostic Command 6.2: Verify server certificate and Central connectivity using the device-identity certificate

```
switch# start-shell
```

```
sudo start_vrf_shell <Central VRF>
OPENSSL_CONF=/usr/lib/ssl-3/openssl-tpm-provider.cnf \
  curl -I -v [-x <Proxy URL>] [--interface <Source IP>] \
  --cert /fs/security/certmgr/certs/device-identity.crt \
  --key /fs/security/certmgr/keys/device-identity.key \
  --ciphers "ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256" \
  --curves "P-256:P-384:P-521" \
  --http1.1 --tls-max 1.2 \
  --use-certmgr-hpe \
  "https://<Central URL>/wss"
```

Example:

```
switch# start-shell
ssudo start_vrf_shell default
OPENSSL_CONF=/usr/lib/ssl-3/openssl-tpm-provider.cnf \
  curl -I -v -x 198.51.100.33:8080 --interface 192.0.2.1 \
   --cert /fs/security/certmgr/certs/device-identity.crt \
   --key /fs/security/certmgr/keys/device-identity.key \
   --ciphers "ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256" \
   --curves "P-256:P-384:P-521" \
   --http1.1 --tls-max 1.2 \
   --use-certmgr-hpe \
  https://test.central.com/wss
```

Expected Output:

```
*   Trying 198.51.100.33:8080...
* Name '192.0.2.1' family 2 resolved to '192.0.2.1' family 2
* Local port: 0
* Connected to 198.51.100.33 (198.51.100.33) port 443
* CONNECT tunnel: HTTP/1.1 negotiated
* allocate connect buffer
* Establish HTTP proxy tunnel to test.central.com:443
> CONNECT test.central.com:443 HTTP/1.1
> Host: test.central.com:443
> User-Agent: curl/8.7.1
> Proxy-Connection: Keep-Alive
>
< HTTP/1.1 200 Connection Established
HTTP/1.1 200 Connection Established
< Proxy-Agent: Squid/7.1
Proxy-Agent: Squid/7.1
<
* CONNECT phase completed
* CONNECT tunnel established, response 200
* ALPN: curl offers http/1.1
* Cipher selection: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
```

```
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS handshake, CERT verify (15):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256 / secp256r1 /
rsaEncryption
* ALPN: server accepted http/1.1
* Server certificate:
*  subject: C=US; ST=California; L=Santa Clara; O=Hewlett Packard Enterprise
Development; OU=Aruba; CN=test.central.com
*  start date: May  7 09:19:17 2025 GMT
*  expire date: May  6 10:19:17 2026 GMT
*  issuer: CN=Test PKI - HPE Aruba Cloud - Aruba Central CA 412; OU=Aruba;
O=Hewlett Packard Enterprise Development; L=Santa Clara; ST=California; C=US
* SSL: using certmgr API
* SSL: Peer presented certificate chain
* SSL: certificate validation successful
*  SSL certificate verify ok.
*   Certificate level 0: Public key type RSA (2048/112 Bits/secBits), signed using
sha256WithRSAEncryption
*   Certificate level 1: Public key type RSA (4096/152 Bits/secBits), signed using
sha256WithRSAEncryption
*   Certificate level 2: Public key type RSA (2048/112 Bits/secBits), signed using
sha256WithRSAEncryption
*   Certificate level 3: Public key type RSA (2048/112 Bits/secBits), signed using
sha256WithRSAEncryption
* using HTTP/1.x
> HEAD /wss HTTP/1.1
> Host: test.central.com
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 502 Bad Gateway
HTTP/1.1 502 Bad Gateway
< Date: Tue, 26 Aug 2025 14:53:58 GMT
Date: Tue, 26 Aug 2025 14:53:58 GMT
< Content-Type: text/html
Content-Type: text/html
< Content-Length: 150
Content-Length: 150
< Connection: keep-alive
Connection: keep-alive
< Strict-Transport-Security: max-age=3600; includeSubDomains
Strict-Transport-Security: max-age=3600; includeSubDomains
< X-Frame-Options: SAMEORIGIN
X-Frame-Options: SAMEORIGIN
< X-Request-Start: t=1756220038.934
X-Request-Start: t=1756220038.934
< X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; mode=block
< allow-cross-namespace-resources: true
allow-cross-namespace-resources: true
< allow-snippet-annotations: true
allow-snippet-annotations: true
< annotations-risk-level: Critical
annotations-risk-level: Critical
<
* Connection #0 to host 198.51.100.33 left intact
```

Evaluation:

- Verify the SSL connection is established successfully.
- Verify certificate validation messages indicate success.
- Receiving an HTTP response confirms certificate-based authentication works.

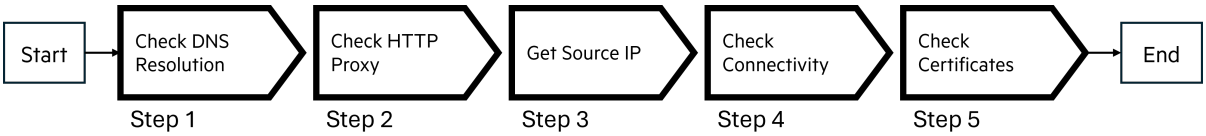
Corrective Action: If certificate validation fails:

- Verify the device certificate is valid and not expired.
- For COP deployments, verify the correct --use-certmgr or --use-certmgr-hpe flag is used.
- Check that the server certificate is valid and not expired.

Scenario: Activate connectivity

The CX switch cannot establish connectivity with the Activate server. The Activate server is used to provision devices and provide the Central location when other sources are not configured.

Troubleshooting Workflow Diagram



Troubleshooting Workflow Steps

Follow the same troubleshooting steps as described in the Central connectivity section, with the following differences:

Server URL: Use https://devices-v2.arubanetworks.com when making HTTPS HEAD requests to test connectivity with the Activate server.

VRF Selection: Try each available VRF until successful DNS resolution and connectivity is established. To list available VRFs, use:

```
switch# start-shell
ovsdb-client dump VRF name

VRF table
name
-------
default
mgmt
```

Test connectivity using each VRF until a successful connection is made.

Scenario: Central remote console shell

Users with admin roles cannot establish a remote console shell (RCS) session from Central to the switch. The RCS feature allows administrators to access the switch CLI directly through SSH from Central for troubleshooting purposes. Connection failures may occur due to network issues, SSH configuration problems, or incompatible security settings.

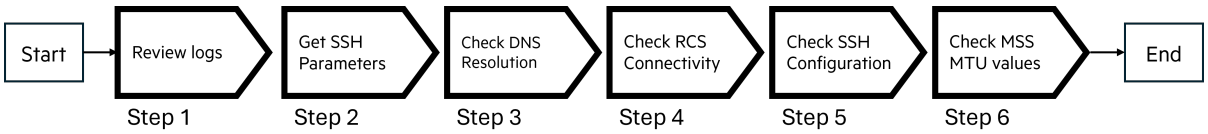
Prerequisites

Enable debug logs

Enable debug logging to capture detailed information about RCS connection attempts:

```
switch# debug sshutils all
switch# debug rest all
```

Troubleshooting Workflow Diagram



Troubleshooting Workflow Steps

Step 1: Review logs for SSH connectivity

Initiate a remote console shell session from Central and review the logs on the switch.

Diagnostic Command:

```
switch# start-shell
journalctl -af -u hpe-restd -u sshd* -u log-proxyd
```

Successful Connection - Expected Output:

```
debug|LOG_INFO|RSSH : id 1, user iap-test, port 443, ssh_port 33484, IP rcs-
test.central.arubanetworks.com, nsName swns, sourceIp 192.0.2.1.
debug|LOG_INFO|RSSH command: [/usr/bin/sshpass -d 3 ssh -tt -o
StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -b 192.0.2.1 -R
33484:localhost:22
iap-test@rcs-test.central.arubanetworks.com -p 443 -vv]
Accepted password for admin from ::1 port 57504 ssh2
pam_unix(sshd:session): session opened for user admin by (uid=0) from ::1
Event|5209|LOG_INFO|CDTR|1|User admin logged in from ::1 through SSH session.
```

Failed Connection - Example Output:

```
debug|LOG_INFO|RSSH : id 1, user iap-test, port 443, ssh_port 33484, IP rcs-
test.central.arubanetworks.com, nsName swns, sourceIp 192.0.2.1.
debug|LOG_INFO|Using proxy ip 198.51.100.33, port 8080
debug|LOG_INFO|RSSH command: [/usr/bin/sshpass -d 3 ssh -tt -o
StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -b 192.0.2.1 -R
33484:localhost:22
iap-test@rcs-test.central.arubanetworks.com -p 443 -vv]
Unable to negotiate with ::1 port 47750: no matching key exchange method found.
Their offer: 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,
ext-info-c,kex-strict-c-v00@openssh.com [preauth]
debug|LOG_DEBUG|Wait returned for /usr/libexec/common/scripts/cgescape is exit
status 255.
debug|LOG_DEBUG|SSH connection logging | OpenSSH_9.6p1, OpenSSL 3.4.0 22 Oct 2024
debug1: cannot process default engine config file: No such file or directory
debug1: Reading configuration data /etc/ssh/ssh_config
```

```
debug1: ssh_set_validator: ignore responder url
debug1: Connecting to rcs-test.central.arubanetworks.com [203.0.113.12] port 443.
debug1: ssh_create_socket: bound to 192.0.2.1
debug1: Connection established.
debug1: Local version string SSH-2.0-OpenSSH_9.6 PKIX[14.4.2]
debug1: Remote protocol version 2.0, remote software version Go
debug1: no match: Go
debug1: x.509 compatibility rfc6187_missing_key_identifier=no: pattern '*' match
'Go'
debug1: x.509 compatibility rfc6187_asn1_opaque_ecdsa_signature=no: pattern '*'
match 'Go'
debug1: x.509 compatibility broken list with accepted publickey algorithms=no:
pattern '*' match 'Go'
debug1: Authenticating to rcs-test.central.arubanetworks.com:443 as 'iap-test'
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: diffie-hellman-group14-sha1
debug1: kex: host key algorithm: rsa-sha2-256
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: rsa-sha2-256
SHA256:U2DN6AjUh24D475uVopix1ihD1nTX7/5zT9P764VhDE
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: checking without port identifier
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
Warning: Permanently added '[rcs-test.central.arubanetworks.com]:443' (RSA) to the
list of known hosts.
debug1: ssh_packet_send2_wrapped: resetting send seqnr 3
debug1: rekey out after 67108864 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: ssh_packet_read_poll2: resetting read seqnr 3
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 67108864 blocks
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<ssh-ed25519,sk-ssh-
ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,ecdsa-sha2-nistp256,ecdsa-
sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-256,rsa-sha2-512,ssh-rsa,ssh-dss>
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: password,publickey
debug1: Next authentication method: publickey
debug1: Next authentication method: password
Authenticated to rcs-test.central.arubanetworks.com ([203.0.113.12]:443) using
"password".
debug1: Remote connections from LOCALHOST:33484 forwarded to local address
localhost:22
debug1: ssh_init_forwarding: expecting replies for 1 forwards
debug1: channel 0: new session [client-session] (inactive timeout: 0)
debug1: Entering interactive session.
debug1: pledge: network
debug1: remote forward success for: listen 33484, connect localhost:22
debug1: forwarding_success: all expected forwarding replies received
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 0 win 2097152 max
32768
```

```
debug1: client_request_forwarded_tcpip: listen localhost port 33484, originator
127.0.0.1 port 35772
debug1: connect_next: start for host localhost ([::1]:22)
debug1: connect_next: connect host localhost ([::1]:22) in progress, fd=7
debug1: channel 1: new forwarded-tcpip [127.0.0.1] (inactive timeout: 0)
debug1: confirm forwarded-tcpip
debug1: channel 1: connected to localhost port 22
debug1: ssh_tty_make_modes: no fd or tio
debug1: pledge: network
debug1: fd 4 clearing O_NONBLOCK
You are connected to RCS Server
Type 'exit' or 'quit' to close the connection
# debug1: fd 5 clearing O_NONBLOCK
debug1: channel 0: free: client-session, nchannels 2
debug1: channel 1: free: 127.0.0.1, nchannels 1
Connection to rcs-test.central.arubanetworks.com closed.
Transferred: sent 2800, received 3976 bytes, in 0.1 seconds
Bytes per second: sent 21911.9, received 31114.9
debug1: Exit status -1
```

Evaluation: Review the logs for error messages indicating the cause of connection failure.

Step 2: Extract SSH parameters from logs

From the logs, identify the SSH connection parameters.

Parameters to Extract:

Parameter	Example Value	Notes
Server URL	rcs-test.central.arubanetworks.com	
Username	iap-test	
Port	443	
Source IP	192.0.2.1	May be empty if not configured
HTTP Proxy IP	198.51.100.33	May be empty if not configured
HTTP Proxy Port	8080	May be empty if not configured

Step 3: Verify DNS resolution

If the RCS server address is an FQDN, verify DNS resolution.

Diagnostic Command:

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
nslookup <Server Address>
```

Example:

```
sudo start_vrf_shell default
nslookup rcs-test.central.arubanetworks.com
```

Evaluation: Verify the DNS query returns a valid IP address.

Corrective Action: If DNS resolution fails, verify DNS server configuration and connectivity.

Step 4: Test connectivity with RCS server

Test SSH connectivity to the RCS server.

Diagnostic Command (without HTTP Proxy):

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
ssh -b <Source IP> <Username>@<Server Address> -p <Port> -vvv
```

Example:

```
switch# start-shell
sudo start_vrf_shell default
ssh -b 192.0.2.1 iap-test@rcs-test.central.arubanetworks.com -p 443 -vvv
```

Diagnostic Command (with HTTP Proxy):

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
ssh -b <Source IP> -o ProxyCommand="/usr/bin/socat - PROXY:<HTTP Proxy
IP>:%h:%p,proxyport=<HTTP Proxy Port>"
<Username>@<Server Address> -p <Port> -vvv
```

Example:

```
sudo start_vrf_shell default
ssh -b 192.0.2.1 -o ProxyCommand="/usr/bin/socat -
PROXY:198.51.100.33:%h:%p,proxyport=8080"
iap-test@rcs-test.central.arubanetworks.com -p 443 -vvv
```

Evaluation: If the command reaches a password prompt, connectivity is successful.

Corrective Action: If connection fails, verify network connectivity, firewall rules and continue with the next steps.

Step 5: Verify SSH server configuration

Verify the SSH server configuration on the switch.

Diagnostic Command:

```
switch# show ssh server all-vrfs
```

Evaluation: Check for the following common configuration issues:

Issue 5.1: SSH server not configured on Central VRF

Corrective Action: Enable SSH server on the same VRF used for Central connectivity:

```
switch# configure
switch(config)# ssh server vrf <VRF>
```

Issue 5.2: SSH server not listening on port 22

The RCS connection requires the SSH server to listen on TCP port 22.

Corrective Action: Configure the SSH server to listen on port 22:

```
switch# configure
switch(config)# ssh server port 22
```

Issue 5.3: SSH server allow list does not include loopback

If the SSH server is configured to allow certain IP addresses to connect, make sure to also allow the IPv6 loopback address (i.e. ::1), as the loopback address is used by the reverse SSH connection.

Corrective Action: Add the IPv6 loopback address to the allow list:

```
switch# configure
switch(config)# ssh server allow-list
switch(config-ssh-al)# ipv6 ::1
switch(config-ssh-al)# enable
```

Issue 5.4: Maximum SSH connections reached

The SSH server allows a maximum of 5 concurrent connections.

Diagnostic Command:

```
switch# show ssh server sessions vrf <VRF>
```

Corrective Action: Close unused SSH sessions to free up connection slots.

Issue 5.5: SSH ciphers not compatible with RCS server

Diagnostic Command:

```
switch# show running-config | include "ssh ciphers"
```

Evaluation: Verify configured ciphers are supported by the RCS server:

Cipher	RCS Support
aes128-ctr	Yes
aes256-ctr	Yes
aes128-gcm@openssh.com	Yes

Cipher	RCS Support
aes256-gcm@openssh.com	Yes
chacha20-poly1305@openssh.com	Yes
aes192-ctr	Yes
aes128-cbc	No
aes256-cbc	No
aes192-cbc	No

Corrective Action: Configure supported ciphers:

```
switch# configure
switch(config)# ssh ciphers <ciphers>
```

Issue 5.6: SSH host key algorithms not compatible with RCS server

Diagnostic Command:

```
switch# show running-config | include "ssh host-key-algorithms"
```

Evaluation: Verify configured algorithms are supported by the RCS server:

Algorithm	RCS Support
rsa-sha2-256	Yes
rsa-sha2-512	Yes
ssh-rsa	Yes
ecdsa-sha2-nistp256	No
ecdsa-sha2-nistp384	No
ecdsa-sha2-nistp521	No
ssh-ed25519	No

Corrective Action: Configure supported algorithms:

```
switch# configure
switch(config)# ssh host-key-algorithms <algorithms>
```

Issue 5.7: SSH key exchange algorithms not compatible with RCS server

Diagnostic Command:

```
switch# show running-config | include "ssh key-exchange-algorithms"
```

Evaluation: Verify configured algorithms are supported by the RCS server:

Algorithm	RCS Support
curve25519-sha256	Yes
curve25519-sha256@libssh.org	Yes
ecdh-sha2-nistp256	Yes
ecdh-sha2-nistp384	Yes
ecdh-sha2-nistp521	Yes
diffie-hellman-group14-sha256	Yes
diffie-hellman-group14-sha1	No
diffie-hellman-group-exchange-sha1	No
diffie-hellman-group-exchange-sha256	No
diffie-hellman-group16-sha512	No
diffie-hellman-group18-sha512	No

Corrective Action: Configure supported algorithms:

```
switch# configure
switch(config)# ssh key-exchange-algorithms <algorithms>
```

Step 6: Verify MSS and MTU values

If network issues are suspected, verify MSS and MTU values are consistent across the network path.

Diagnostic Command:

Review current MTU configuration and validate with network infrastructure to ensure all devices in the path support the configured values.

Corrective Action: Adjust MTU values if mismatches are identified in the network path.

Scenario: Central disconnection timeout

The switch experiences delayed disconnection from Central or the hpe-restd service becomes unresponsive during a disconnection event. This may occur during:

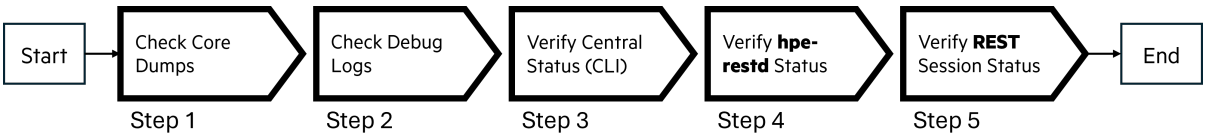
- Network interface flapping on the interface used for Central connectivity
- Central server upgrades or maintenance

- Manual disable/enable of the hpe-anw-central feature
- Disconnection from external clients (NetEdit or WebUI)

Symptoms include:

- hpe-restd does not respond to configuration changes
- Switch fails to reconnect to Central within the expected timeframe
- After 12 minutes, hpe-restd automatically restarts with a timeout message

Troubleshooting Workflow Diagram



Troubleshooting Workflow Steps

Step 1: Check for core dumps

Verify if the hpe-restd service has generated core dumps.

Diagnostic Command:

```
switch# show core-dump all
```

Evaluation: If core dumps are present, note the timestamp and proceed with the remaining steps.

Step 2: Review debug logs

Check if the disconnection timeout mechanism was triggered.

Diagnostic Command:

```
switch# show debug buffer module central | inc "hpe-restd did not close the
connection to Central
after: 12 minutes, restarting service"
```

Evaluation: If this message is present, the timeout mechanism was triggered and the service should have automatically restarted to restore connectivity.

Step 3: Verify Central connection status via CLI

Check the current Central connection status.

Diagnostic Command:

```
switch# show hpe-anw-central
```

Evaluation: The Central connection status may show:

- connected: Connection appears established (verify with next steps).
- connection_failure: Connection has failed.
- N/A: Status is unavailable.

Step 4: Verify Central status in hpe-restd

Check the internal Central connection status in the hpe-restd service.

Diagnostic Command:

```
switch# start-shell
sudo ovs-appctl -t hpe-restd central/show --state
```

Evaluation: If the status shows connected when Central connectivity is not working, the service may be waiting for internal processes to complete the disconnection.

Step 5: Verify WebSocket connection status

Check if an active WebSocket connection exists.

Diagnostic Command:

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
netstat -ntp
```

Evaluation: Look for active connections to the Central IP address. If the Central connection is present when it should be disconnected, the disconnection process is incomplete.

Step 6: Verify REST session status

Check if a persistent REST session exists for Central.

Diagnostic Command:

```
switch# start-shell
sudo start_vrf_shell <Central VRF>
```

Evaluation: Look for a row with the PERSISTENT column set to True. This indicates the Central session still exists and the disconnection is incomplete.

Step 7: Collect diagnostic information

If the issue persists, collect comprehensive diagnostic information.

Corrective Actions:

1. Save the output of all diagnostic commands from the previous steps.
2. Generate support files without rebooting the switch to preserve diagnostic state:

```
switch# copy support-files
```

3. Contact HPE support and provide:

- Collected command outputs.
- Support files.
- Description of when the issue occurred.
- Any recent configuration changes.

Workaround

If hpe-restd is unresponsive and has not automatically restarted, manually restart the service.

Corrective Action:

```
switch# https-server session close all
```

This command closes all HTTPS server sessions and triggers a restart of the **hpe-restd** service, which should restore normal operation.

Related features

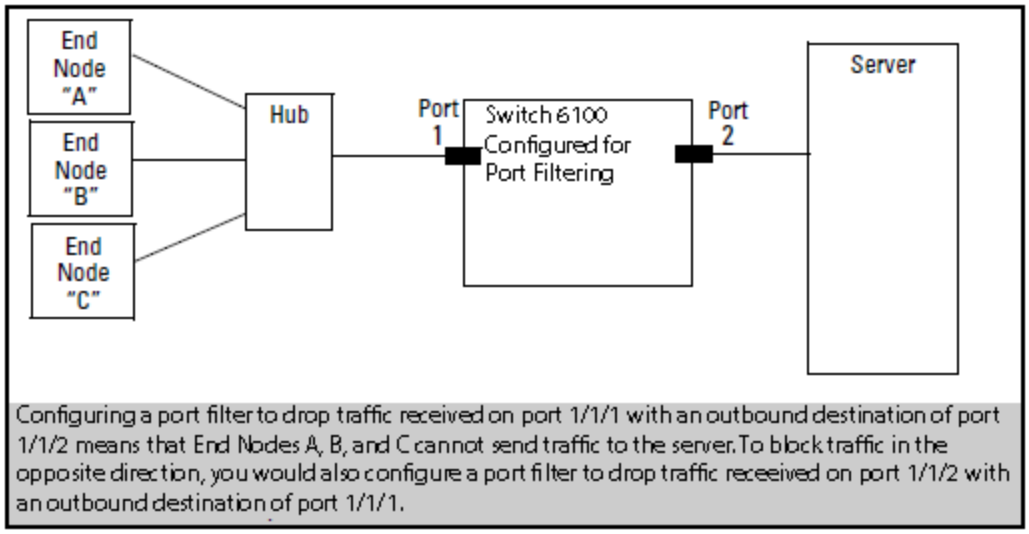
When configuring the CX device for Central connectivity, it might also be necessary to configure the following features:

Feature	Reason
DNS	Used to translate the Central and/or Activate hostnames into IPv4 and/or IPv6 addresses
HTTP Proxy	Used as a gateway between the CX Device and/or Central and Activate servers
Zero Touch Provisioning	Used to receive the Central location via DHCP options when the switch boots
Source interface selection	Used to define the outgoing interface from which the connection to Central and/or Activate is established

Chapter 14
Port filtering

Port filtering is a feature in which packets that are ingressed through a source port can be blocked for egressing on a specific set of ports.

Figure 1 *Port Filter Application*



Configuring a port filter to drop traffic received on port 1/1/1 with an outbound destination of port 1/1/2 means that End Nodes A, B, and C cannot send traffic to the server. To block traffic in the opposite direction, you would also configure a port filter to drop traffic receeived on port 1/1/2 with an outbound destination of port 1/1/1.

;" />

Port filtering commands

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
```

Command History

Release	Modification
10.14	Added information related to role based IPFIX.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

show portfilter

`show portfilter [<IFNAME>][vsx-peer]`

Description

Displays filter settings for all interfaces or a specific interface.

Parameter	Description
<IFNAME>	Specifies the ingress interface name. Specifies one of these values: ■ *<FQDN>*: a fully qualified domain name. ■ *<IPV4>*: an IPv4 address. ■ *<IPV6>*: an IPv6 address.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	Operator (>) or Manager (#)	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 15
DNS

The Domain Name System (DNS) is the Internet protocol for mapping domain names or hostnames into IPv4 and/or IPv6 addresses. DNS allows users to enter more readily memorable and intuitive hostnames, rather than IP addresses, to identify devices connected to a network. It also allows a host to keep the same hostname even if it changes its IP address.

Hostname resolution can be either static or dynamic.

- In static resolution, a local table is defined on the switch that associates hostnames with their IP addresses. Static tables can be used to speed up the resolution of frequently queried hosts.
- Dynamic resolution requires that the switch query a DNS server located elsewhere on the network. Dynamic name resolution takes more time than static name resolution, but requires far less configuration and management.

Configuration

VxLAN IPv4 and IPv6 underlay support the DNS client. To ensure configuration, make sure the following are set up:

- VxLAN overlay
  - Must be configured to establish the VxLAN tunnel.
- VxLAN tunnel
  - Ensure the tunnel is established between the VTEPS via either static or EVPN using the following command: **show interface VxLAN VTEPS**.

For more information, refer to the AOS-CX VxLAN EVPN Guide.

DNS client

The DNS client resolves hostnames to IP addresses for protocols that are running on the switch. When the DNS client receives a request to resolve a hostname, it can do so in one of two ways:

- Forward the request to a DNS name server for resolution.
- Reply to the request without using a DNS name server, by resolving the name using a statically defined table of hostnames and their associated IP addresses.

Configuring the DNS client

Procedure

1. Configure one or more DNS name servers with the command `ip dns server`.

2. To resolve DNS requests by appending a domain name to the requests, either configure a single domain name with the command `ip dns domain-name`, or configure a list of up to six domain names with the command `ip dns domain-list`.
3. To use static name resolution for certain hosts, associate an IP address to a host with the command `ip dns host`.
4. Review your DNS configuration settings with the command `show ip dns`.

Examples

This example creates the following configuration:

- Defines the domain **switch.com** to append to all requests.
- Defines a DNS server with IPv4 address of **1.1.1.1**.
- Defines a static DNS host named **myhost1** with an IPv4 address of **3.3.3.3**.
- DNS client traffic is sent on the default VRF (named **default**).

```
switch(config)# ip dns domain-name switch.com
switch(config)# ip dns server-address 1.1.1.1
switch(config)# ip dns host myhost1 3.3.3.3
switch(config)# exit
switch# show ip dns

VRF Name : vrf_mgmt

Host Name                                                                Address
-------------------------------------------------------------------------------


VRF Name : vrf_default
Domain Name : switch.com
DNS Domain list :
Name Server(s) : 1.1.1.1

Host Name                                                                Address
-------------------------------------------------------------------------------
myhost1
```

This example creates the following configuration:

- Defines three domains to append to DNS requests **domain1.com**, **domain2.com**, **domain3.com** with traffic forwarding on VRF **mainvrf**.
- Defines a DNS server with an IPv6 address of **c::13**.
- Defines a DNS host named **myhost** with an IPv4 address of **3.3.3.3**.

```
switch(config)# ip dns domain-list domain1.com vrf mainvrf
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain3.com vrf mainvrf
switch(config)# ip dns server-address c::13
switch(config)# ip dns host myhost 3.3.3.3 vrf mainvrf
switch(config)# quit
switch# show ip dns mainvrf

VRF Name : mainvrf
Domain Name :
DNS Domain list : domain1.com, domain2.com, domain3.com
```

```
Name Server(s) : c::13

Host Name                                                                    Address
-------------------------------------------------------------------------------------
myhost                                                                       3.3.3.3
```

DNS client commands

ip dns domain-list

```
ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
no ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
```

Description

Configures one or more domain names that are appended to the DNS request. The DNS client appends each name in succession until the DNS server replies. Domains can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF.

The **no** form of this command removes a domain from the list.

Parameter	Description
`list <DOMAIN-NAME>`	Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.
`vrf <VRF-NAME>`	Specifies a VRF name. Default: default.

Examples

This example defines a list with two entries: **domain1.com** and **domain2.com**.

```
switch(config)# ip dns domain-list domain1.com
switch(config)# ip dns domain-list domain2.com
```

This example defines a list with two entries, **domain2.com** and **domain5.com**, with requests being sent on **mainvrf**.

```
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain5.com vrf mainvrf
```

This example removes the entry **domain1.com**.

```
switch(config)# no ip dns domain-list domain1.com
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 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>][vsx-peer]`

Description

Shows all DNS client configuration settings or the settings for a specific VRF.

Parameter	Description
`vrf <VRF-NAME>`	Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

DNS client arbitration on the MGMT interface on a MGMT VRF can be updated via three different methods.

1. Using the **domain-name <name>** or **nameservers <servers>** commands in the command-line interface.
2. Using the **ip dns domain-name *<DOMAIN-NAME>* vrf *MGMT*** or **ip dns server-address <SERVER> vrf MGMT** commands in the command-line interface.
3. Using the **ip dhcp** command in the command-line interface (dynamic enties).

AOS-CX gives the following priority levels to the these three update methods.

- Priority 1 - standalone CLI configuration
- Priority 2 - static ip dns configuration
- Priority 3 - Dynamic config

Examples

These examples define DNS settings and then show how they are displayed with the **show ip dns** command.

```
switch(config)# ip dns domain-name domain.com
switch(config)# ip dns domain-list domain5.com
switch(config)# ip dns domain-list domain8.com
switch(config)# ip dns server-address 4.4.4.4
switch(config)# ip dns server-address 6.6.6.6
switch(config)# ip dns host host3 5.5.5.5
switch(config)# ip dns host host2 2.2.2.2
switch(config)# ip dns host host3 c::12
switch(config)# ip dns domain-name reddomain.com vrf red
switch(config)# ip dns domain-list reddomain5.com vrf red
switch(config)# ip dns domain-list reddomain8.com vrf red
switch(config)# ip dns server-address 4.4.4.5 vrf red
switch(config)# ip dns server-address 6.6.6.7 vrf red
switch(config)# ip dns host host3 5.5.5.6 vrf red
switch(config)# ip dns host host2 2.2.2.3 vrf red
switch(config)# ip dns host host3 c::13 vrf red
switch# show ip dns
VRF Name : default

Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6

Host Name    Address
```

```
--------------------------------
host2            2.2.2.2
host3            5.5.5.5
host3            c::12
VRF Name : red

Domain Name : reddomain.com
DNS Domain list : reddomain5.com, reddomain8.com
Name Server(s) : 4.4.4.5, 6.6.6.7

Host Name    Address
--------------------------------
host2            2.2.2.3
host3            5.5.5.6
host3            c::13
```

```
switch(config)# ip dns domain-name domain.com vrf red
switch(config)# ip dns domain-list domain5.com vrf red
switch(config)# ip dns domain-list domain8.com vrf red
switch(config)# ip dns server-address 4.4.4.4 vrf red
switch(config)# ip dns server-address 6.6.6.6 vrf red
switch(config)# ip dns host host3 5.5.5.5 vrf red
switch(config)# no ip dns host host2 2.2.2.2 vrf red
switch(config)# ip dns host host3 c::12 vrf red

switch# show ip dns vrf red
VRF Name : red

Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6

Host Name    Address
--------------------------------
host3            5.5.5.5
host3            c::12
```

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.

Chapter 16
Device discovery and configuration

The switch provides support for LLDP and CDP to enable automatic discovery and configuration of other devices on the network.

Device Profile Usage Considerations

The following behaviors and limitations should be taken into consideration when configuring a device profile on Link Aggregation Group (LAG) or Multi-chassis Link Aggregation Group (MCLAG).

Device Profiles on LAG and MCLAG

- When using Device profile to onboard a device with multiple interfaces (such as a dual port AP) over a LAG, set the authentication mode in the role applied to the device to **device-mode**. The **multi-domain** authentication mode is not supported with a device profile on a LAG.
- When using Device profile to onboard a device on MCLAG port, set the authentication mode in the role applied to the device to **device-mode** or **proxy-mode**. The **multi-domain** and **client-mode** authentication mode is not supported with device profile on MCLAG.
- It is not recommended to connect different devices to the same LAG when using a device profile on the LAG.
- When updating a LAG membership, all the device profile clients on the LAG are logged off automatically from the switch and from both peers on MCLAG port.
- If you issue the command **aaa authentication port-access allow-cdp-proxy-logoff** on the LAG, a proxy-logoff TLV received on any member interface of the LAG will log off all clients onboarded on the LAG.
- Depending on resource availability or auth/role application status on each peer, the same MAC may be allowed in one peer and denied in another for a MAC learned on MCLAG port.

Security Considerations

- Each individual interface of a LAG must successfully match a Device profile for the corresponding interface to be unblocked on the data plane.
- An onboarded client on the LAG is authorized to send and receive packets on any of the member interface of the LAG that is unblocked on the data plane. This is true even for a different client connected to the same LAG.
- When using LLDP packets to authenticate a device using a device profile on a LAG, issue the command **aaa authentication port-access allow-lldp-auth mac chassis-mac** to set the authentication MAC address as the chassis MAC address
- LLDP BPDUs are blocked by default. Issue the command **aaa authentication port-access allow-lldp-bpdu** to allow the LLDP BPDUs.
- If a Device profile is used to onboard multiple devices connected to the same LAG, the client limit on the LAG must be configured to match the number of clients onboarding the LAG.
- When using LLDP packets to authenticate a Dual Port AP using a device profile on a LAG, issue the command **aaa authentication port-access allow-lldp-auth mac source-mac** to set the authentication MAC address as the port/interface MAC address.

Supported Role Attributes

The following port-access role attributes are supported for clients that onboard via device profile on a LAG.

- Authentication mode
- Client inactivity timeout
- Session timeout
- Access and Trunk VLANs
- Port-Access policy (not supported on MCLAG)
- MTU
- PoE Priority
- PoE Allocate-By
- Private-VLAN
- STP admin edge port
- Trust mode
- GBP role

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
```

Command History

Release	Modification
10.13	(for 8100 and 8360 Switch Series only) This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	`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
      no routing
    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       : hpe-anw-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
   no routing
    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
```

Command History

Release	Modification
10.13	(for HPE Aruba Networking 8100 and 8360 Switch Series only) This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	`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
no routing
    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
```

Command History

Release	Modification
10.13	(for 8100 and 8360 Switch Series only) This command can be issued from a Link Aggregation Group (LAG) context.
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8360	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
    no routing
    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
    no routing
    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
```

Command History

Release	Modification
10.13	(for 8100 and 8360 Switch Series only) This command can be issued from a Link Aggregation Group (LAG) context.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8360	`config-if` `config-lag-if`	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables device profile on the port. By default, device profile is already enabled on the port.,

The **no** form of this command disables device profile on the port.

Examples

Enabling a device profile on port 1/1/1 and disabling on lag 1:

```
switch(config)# interface 1/1/1
switch(config-if)# port-access device-profile
switch(config-if-deviceprofile)#
enable  Enable device-profile on this port.
mode    Configure device-profile mode for this port.
switch(config-if-deviceprofile)# enable
switch(config-if-deviceprofile)# end
```

```
switch(config)# interface lag 1
switch(config-lag-if)# port-access device-profile
switch(config-lag-if-deviceprofile)# no
enable  Enable device-profile on this port.
mode    Configure device-profile mode for this port.
switch(config-lag-if-deviceprofile)# no enable
switch(config-lag-if-deviceprofile)# end
```

Showing running configuration:

```
switch#
switch# show running-config
interface lag 1
   no shutdown
   no routing
   vlan access 1
   port-access device-profile
     no enable

interface 1/1/1
```

```
no shutdown
no routing
vlan access 1
exit
```

Command History

Release	Modification
10.17	Command introduced

Command Information

Platforms	Command context	Authority
8100 8360	`config-device-profile`	Administrators or local user group members with execution rights for this command.

LLDP

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) provides a standards-based method for network devices to discover each other and exchange information about their capabilities. An LLDP device advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets on all interfaces on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports on which inbound LLDP is enabled. Inbound packets from neighbor devices are stored in a special LLDP MIB (management information base). This information can then be queried by other devices through SNMP.

LLDP information is used by network management tools to create accurate physical network topologies by determining which devices are neighbors and through which interfaces they connect. LLDP operates at layer 2 and requires an LLDP agent to be active on each interface that sends and receives LLDP advertisements. LLDP advertisements can contain a variable number of TLV (type, length, value) information elements. Each TLV describes a single attribute of a device such as: system capabilities, management IP address, device ID, port ID.

Packet boundaries

When multiple LLDP devices are directly connected, an outbound LLDP packet travels only to the next LLDP device. An LLDP-capable device does not forward LLDP packets to any other devices, regardless of whether they are LLDP-enabled.

An intervening hub or repeater forwards the LLDP packets it receives in the same manner as any other multicast packets it receives. Therefore, two LLDP switches joined by a hub or repeater handle LLDP traffic in the same way that they would if directly connected.

Any intervening 802.1D device or Layer-3 device that is either LLDP-unaware or has disabled LLDP operation drops the packet.

LLDP-MED

LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. LLDP-MED in the switches uses the standard LLDP commands described earlier in this section, with some extensions, and also introduces new commands unique to

LLDP-MED operation. The show commands described elsewhere in this section are applicable to both LLDP and LLDP-MED operation. LLDP-MED enables:

- Configure Voice VLAN and advertise it to connected MED endpoint devices.
- Power over Ethernet (PoE) status and troubleshooting support via SNMP.

LLDP agent

When you enable LLDP on the switch, it is automatically enabled on all data plane interfaces. You can customize this behavior by manually enabling/disabling support on each interface.

Supported standards

The LLDP agent supports the following standards: IEEE 802.1AB-2005, Station, and Media Access Control Connectivity Discovery.

Supported interfaces

LLDP is supported on interfaces mapped to a physical port, and the Out-Of-Band Management (OOBM) port. It is not supported on logical interfaces, such as loopback, tunnels, and SVIs.

Operating modes

When LLDP is enabled, the switch periodically transmits an LLDP advertisement (packet) out each active port enabled for outbound LLDP transmissions and receives LLDP advertisements on each active port enabled to receive LLDP traffic.

The LLDP agent can operate in one of the following modes:

- Transmit and receive (TxRx): This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets and to store the data from received (inbound) LLDP packets in the switch's MIB.
- Transmit only (Tx): Enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.
- Receive only (Rx): Enables a port to receive and read LLDP packets from LLDP neighbors and to store the packet data in the switch's MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.
- Disabled: Disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.

An LLDP agent operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes.

Sending LLDP frames

Each time the LLDP operating mode of an LLDP agent changes, its LLDP protocol state machine reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, an LLDP agent must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.

Receiving LLDP frames

An LLDP agent operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the LLDP agent saves the information and starts an aging

timer. The initial value of the aging timer is equal to the TTL value in the Time To Live TLV carried in the LLDP frame. When the LLDP agent receives a new LLDP frame, the aging timer restarts. When the aging timer decreases to zero, all saved information ages out.

TLV support

By default, the agent sends and receives the following mandatory TLVs on each interface:

- Port ID
- Chassis ID
- TTL

By default, the following ANSI/TIA-1057 TLVs for LLDP Media Endpoint Discovery (MED) are enabled on an agent. Sending them depends on the configuration and reception of any MED TLVs:

- MAC/PHY status. Includes the bit rate and auto negotiation status of the link.
- Power Via MDI: Includes Power Over Ethernet related information for supported interfaces.
- Port description
- System name
- System description
- Management address
- System capabilities
- Port VLAN ID

By default, the agent sends and receives the following ANSI/TIA-1057 TLVs for LLDP Media Endpoint Discovery (MED):

- Capabilities: Indicates MED TLV capability.
- Power Via MDI: Includes Power Over Ethernet related information.
- Network Policy: Includes the VLAN configuration for voice application.
- Location: Location identification information.
- Extended Power Via MDI: Power Over Ethernet related information

TLV advertisements

The LLDP agent transmits the following:

- Chassis-ID: Base MAC address of the switch.
- Port-ID: Port number of the physical port.
- Time-to-Live (TTL): Length of time an LLDP neighbor retains advertised data before discarding it.
- System capabilities: Identifies the primary switch capabilities (bridge, router). Identifies the primary switch functions that are enabled, such as routing.
- System description: Includes switch model name and running software version, and ROM version.
- System name: Name assigned to the switch.
- Management address: Default address selection method unless an optional address is configured.
- Port description: Physical port identifier.
- Port VLAN ID: On an L2 port, contains access or native VLAN ID. On an L3 port, contains a value of 0. Trunk allowed VLANs information are not advertised as part of the Port VLAN ID TLV. (Not supported on the OOBM interface)

- Port VLAN Name: Access or native VLAN name. Enabled by default.
- Port MFS: Maximum Frame Size. Enabled by default.

LLDP MED support

LLDP-MED interoperates with directly connected IP telephony (endpoint) clients and provides the following features:

- Advertisement of the voice VLAN configured on the interface which is used by connected IP telephony (endpoint) clients.
- Advertisement of the configured location on the switch that can be used by the connected endpoint.
- Support for the fast-start capability

LLDP-MED is intended for use with VoIP endpoints and is not designed to support links between network infrastructure devices (such as switch-to-switch or switch-to-router links).

LLDP EEE

Energy Efficient Ethernet (EEE) is a mechanism defined by IEEE 802.3az, which is an extension of 802.3 IEEE standards. EEE defines support for the device to operate in the Low Power Idle (LPI) mode during low link utilization. This allows both sides of a link to disable or turn off respective transmit/receive circuitry to save power. EEE uses LLDP for exchanging optimal set of parameters for both devices.

Guidelines

- An LLDP must not contain more than one EEE TLV.
- LLDP may or may not be enabled on the interfaces supporting EEE. If LLDP is not enabled, it might not be in the optimal operational mode.
- EEE TLV should not be exchanged until it negotiates from L1 and it detects peer EEE capabilities.
- EEE TLV is disabled by default and enabled only when EEE is active.
- EEE and EEE TLV exchange can be enabled or disabled at the interface level.

Configuring the LLDP agent

Procedure

1. By default, the LLDP agent is enabled on all active interfaces. If LLDP was disabled, enable it with the command `lldp`.
2. By default, the LLDP agent transmits and receive on all interfaces. To customize LLDP behavior on a specific interface, use the commands `lldp transmit` and `lldp receive`.
3. By default, the LLDP agent sets the management address in all TLVs in the following order:
   a. LLDP management IP address.
   b. Loopback interface IP.
   c. ROP (L3 ports) or SVI (L2 ports).
   d. OOBM (Management interface IP).
   e. Base MAC.

   On the OOBM port, the following order is used:

a. LLDP management IP address,
b. IP address of the management interface (OOBM port).
c. IP address of the loopback interface.
d. Base MAC address of the switch.

To specify a different address, use the commands `lldp management-ipv4-address` and `lldp management-ipv6-address`

4. By default, all supported TLVs are sent and received. To customize the list, use the command `lldp select-tlv`.
5. By default, support for the LLDP-MED TLV is enabled. To customize settings, use the commands `lldp med` and `lldp med-location`.
6. If required, adjust LLDP timer, holdtime, reinitialization delay, and transmit delay from their default values with the commands `lldp timer`, `lldp holdtime`, `lldp reinit`, and `lldp txdelay`.

Example

This example creates the following configuration:

- Enables LLDP support.
- Disables LLDP transmission on interface **1/1/1**.

```
switch(config)# lldp
switch(config)# interface 1/1/1
switch(config-copp)# no lldp transmit
```

LLDP commands

clear lldp neighbors

`clear lldp neighbors`

Description

Clears all LLDP neighbor details.

Examples

Clearing all LLDP neighbor details:

```
switch# clear lldp neighbors
```

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

Platforms	Command context	Authority
		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
```

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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

lldp dot3

```
lldp dot3 {poe | macphy}
no lldp dot3 {poe | macphy}
```

Description

Sets the 802.3 TLVs to be advertised. By default, advertisement of both POE and MAC/PHY TLVs is enabled. Not supported on the OOBM interface.

The **no** form of this command disables advertisement of 802.3 TLVs.

Parameter	Description
`poe`	Specifies advertisement of power over Ethernet data link classification.
`macphy`	Specifies advertisement of media access control and physical layer information.

Examples

Enabling advertisement of the POE TLV:

```
switch(config-if)# lldp dot3 poe
```

Disabling advertisement of the POE TLV:

```
switch(config-if)# no lldp dot3 poe
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

lldp dot3 mfs

```
lldp dot3 mfs
no lldp dot3 mfs
```

Description

Enables the 802.3 TLV list in LLDP to advertise for maximum frame size (MFS). Enabled by default.

The **no** form of this command disables the advertisement of maximum frame size TLVs.

Examples

Enabling advertisement of maximum frame size TLVs:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp dot3 mfs
```

Disabling advertisement of maximum frame size TLVs:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp dot3 mfs
```

Command History

Release	Modification
10.11	Command introduced

Command Information

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

lldp 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
```

Command History

Release	Modification
10.12	Command introduced.

Command Information

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

lldp management-ip-address

```
lldp management-ip-address <IPV-ADDR>
no lldp management-ip-address
```

Description

Defines the IP management address of the switch which is sent in the management address TLV. One IPv4 and one IPv6 management address can be configured.

If you do not define an LLDP management address, then LLDP uses one of the following (in order):

- IP address of the port
- IP address of the management interface
- Base MAC address of the switch

The **no** form of this command removes the IPv4 management address of the switch.

Parameter	Description
<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
```

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 the port
- IP address of the management interface
- Base MAC address of the switch

The **no** form of this command removes the IPv6 management address of the switch.

Parameter	Description
<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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

lldp med

```
lldp med [poe [priority-override] | capability | network-policy]
no med [poe [priority-override] | capability | network-policy]
```

Description

Configures support for the LLDP-MED TLV. LLDP-MED (media endpoint devices) is an extension to LLDP developed by TIA to support interoperability between VoIP endpoint devices and other networking end-devices. The switch only sends the LLDP MED TLV after receiving a MED TLV from and connected endpoint device.

Not supported on the OOBM interface.

The **no** form of this command disables support for the LLDP MED TLV.

Parameter	Description
`poe [priority-override]`	Specifies advertisement of power over Ethernet data link classification. The **priority-override** option overrides user-configured port priority for Power over Ethernet. When both **lldp dot3 poe** and **lldp med poe** are enabled, the **lldp dot3 poe3** setting takes precedence. Default: enabled.
`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
```

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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

lldp receive

```
lldp receive
no lldp receive
```

Description

Enables reception of LLDP information on an interface. By default, LLDP reception is enabled on all active interfaces, including the OOBM interface.

The **no** form of this command disables reception of LLDP information on an interface.

Examples

Enabling LLDP reception on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp receive
```

Disabling LLDP reception on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp receive
```

Enabling LLDP reception on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# lldp receive
```

Disabling LLDP reception on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# no lldp receive
```

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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

lldp select-tlv

```
lldp select-tlv <TLV-NAME>
no lldp select-tlv <TLV-NAME>
```

Description

Selects a TLV that the LLDP agent will send and receive. By default, all supported TLVs are sent and received.

The **no** form of this command stops the LLDP agent from sending and receiving a specific TLV.

LLDP supports Organization Unique Identifiers (OUIs) with the following Organization-specific TLVs:

- IEEE 802.1 (DOT1) (oui:0x00, 0x80, 0xc2)
- IEEE 802.3 (DOT3) (oui:0x00, 0x12, 0x0f)
- HPE Aruba Networking (oui:0x88, 0x3a, 0x30)

Parameter	Description
`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. IP address of the lowest configured loopback interface. 3. If layer 3, then the route-only port IP address. If layer 2, the IP address of the SVI. 4. OOBM interface IP address. 5. 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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

lldp tlv-enable

```
lldp tlv-enable basic-tlv management-address-tlv {ip <X.X.X.X>}|{ipv6 <X:X::X:X>}
no lldp select-tlv <TLV-NAME>
```

Description

A **TLV** is an information element that contains the type, length, and value fields. This command configures the IPv4/IPv6 address to be advertised in the management address TLV. This configured value will take the highest precedence in the selection logic the switch uses to identify the IP address to be advertised in the management address TLV.

Parameter	Description
ip <X.X.X.X>	Specify an IP address in IPv4 format **(X.X.X.X**), where **X** is a decimal number from 0 to 255.
ipv6 <X:X::X:X>	Specify an IP address in IPv6 format (**x:x::x:x**), where **X** is a hexadecimal number from **0** to **F**.

Examples

Configuring an IP address in IPv4 format:

```
switch(config)# interface 1/3/1
switch(config-if)# lldp tlv-enable basic-tlv management-address-tlv ip 10.0.0.1
```

Configuring an IP address in IPv6 format:

```
switch(config)# interface 1/3/1
switch(config-if)# lldp tlv-enable basic-tlv management-address-tlv ipv6
2001:db8:85a3::8a2e:370:7334
```

Command History

Release	Modification
10.14.1000	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	`config-if`	Administrators or local user group members with execution rights for this command.

lldp transmit

```
lldp transmit
no lldp transmit
```

Description

Enables transmission of LLDP information on specific interface. By default, LLDP transmission is enabled on all active interfaces, including the OOBM interface.

The **no** form of this command disables transmission of LLDP information on an interface.

Examples

Enabling LLDP transmission on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp transmit
```

Disabling LLDP transmission on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp transmit
```

Enabling LLDP transmission on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# lldp transmit
```

Disabling LLDP transmission on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# no lldp transmit
```

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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show lldp configuration

`show lldp configuration [<INTERFACE-ID>][vsx-peer]`

Description

Shows LLDP configuration settings for all interfaces or a specific interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing configuration settings for all interfaces:

```
switch# show lldp configuration

LLDP Global Configuration
=========================
LLDP Enabled                 : No
LLDP Transmit Interval       : 30
LLDP Hold Time Multiplier    : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval   : 2
LLDP Trap Enabled            : No

TLVs Advertised
===============
Management Address
```

```
Port Description
Port VLAN-ID
System Description
System Name

LLDP Port Configuration
=======================
PORT            TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-------------------------------------------------------------------------
1/1/1           Yes                 Yes                 Yes
1/1/2           Yes                 Yes                 Yes
1/1/3           Yes                 Yes                 Yes
1/1/4           Yes                 Yes                 Yes
1/1/5           Yes                 Yes                 Yes
1/1/6           Yes                 Yes                 Yes
...........
...........
mgmt            Yes                 Yes                 Yes
```

This example shows configuration settings for interface **1/1/1**.

```
switch# show lldp configuration 1/1/1

LLDP Global Configuration
=========================
LLDP Enabled                 : Yes
LLDP Transmit Interval       : 30
LLDP Hold Time Multiplier    : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval   : 2
LLDP Trap Enabled            : No

LLDP Port Configuration
=======================
Auto Flush On Link Down      : Yes
Management IPv4 Address      : 10.1.1.1
Management IPv6 Address      : 3001:1::1:1
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
```

Command History

Release	Modification
10.14.1000	When displaying the LLDP configuration for a specific interface, the output of this command displays any configured management IP addresses.
10.07 or earlier	--

Command Information

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

show lldp configuration mgmt

```
show lldp configuration mgmt
```

Description

Shows LLDP configuration settings for the OOBM interface.

Example

Showing configuration settings for all interfaces:

```
switch# show lldp configuration mgmt

LLDP Global Configuration
=========================
LLDP Enabled                 : Yes
LLDP Transmit Interval       : 30
LLDP Hold Time Multiplier    : 4
LLDP Transmit Delay Interval : 2
LLDP Reinit Timer Interval   : 2
LLDP Trap Enabled            : Yes


LLDP Port Configuration
=======================
PORT           TX-ENABLED          RX-ENABLED          INTF-TRAP-ENABLED
-------------------------------------------------------------------------
mgmt           Yes                 Yes                 Yes
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp local-device

```
show lldp local-device[vsx-peer]
```

Description

Shows global LLDP information advertised by the switch, as well as port-based data. If VLANs are configured on any active interfaces, the VLAN ID is only shown for trunk native or untagged VLAN IDs on access interfaces.

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

Example

Showing global LLDP information only (all ports including OOBM port are administratively down):

```
switch# show lldp local-device

Global Data
===========

Chassis-ID             : 1c:98:ec:e3:45:00
System Name            : switch
System Description     : HPE ANW JL375A 8400X XL.01.01.0001
Management Address     : 192.168.10.1
Capabilities Available : Bridge, Router
Capabilities Enabled   : Bridge, Router
TTL                    : 120
```

Showing all ports except **1/1/11** and OOBM as administratively down:

```
switch# show lldp local-device

Global Data
===========

Chassis-ID             : 1c:98:ec:e3:45:00
System Name            : switch
System Description     : HPE ANW
Management Address     : 192.168.10.1
Capabilities Available : Bridge, Router
Capabilities Enabled   : Bridge, Router
TTL                    : 120

Port Based Data
===============

Port-ID           : 1/1/11
Port-Desc         : "1/1/11"
Port Mgmt-Address : 164.254.21.220
Port VLAN ID      : 1

Port-ID           : mgmt
Port-Desc         : "mgmt"
Port Mgmt-Address : 164.254.21.220
```

In this example, all the ports except **1/1/11** are administratively down, and VLAN ID 100 is configured on this access interface.

```
switch# show lldp local-device

Global Data
===========

Chassis-ID              : 1c:98:ec:e3:45:00
System Name             : switch
System Description      : HPE ANW
Management Address      : 192.168.10.1
Capabilities Available : Bridge, Router
Capabilities Enabled    : Bridge, Router
TTL                     : 120

Port Based Data
===============

Port-ID           : 1/1/11
Port-Desc         : "1/1/11"
Port VLAN ID      : 100
Parent Interface  : interface 1/1/11
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show lldp neighbor-info

`show lldp neighbor-info [<INTERFACE-NAME>][vsx-peer]`

Description

Displays information about neighboring devices for all interfaces or for a specific interface. The information displayed varies depending on the type of neighbor connected and the type of TLVs sent by the neighbor.

Parameter	Description
<INTERFACE-NAME>	Specifies the interface for which to show information for neighboring devices. Use the format **member/slot/port** (for example, **1/3/1**).
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing LLDP information for all interfaces:

```
switch# show lldp neighbor-info

LLDP Neighbor Information
=========================

Total Neighbor Entries          : 3
Total Neighbor Entries Deleted  : 0
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 0

LOCAL-PORT  CHASSIS-ID         PORT-ID       PORT-DESC     TTL      SYS-NAME
-------------------------------------------------------------------------------
1/1/1       70:72:cf:a4:7d:50  1/1/1         1/1/1         32       switch
1/1/2       48:0f:cf:af:73:80  1/1/2         1/1/2         120      switch
1/1/46      48:0f:cf:af:73:80  1/1/46        1/1/46        120      switch
mgmt        48:0f:cf:af:73:80  mgmt          mgmt          120      switch
```

Showing information for interface **1/3/1** when it has only one switch connected as a neighbor:

```
switch# show lldp neighbor-info 1/3/1

Port                           : 1/1/1
Neighbor Entries               : 1
Neighbor Entries Deleted       : 0
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 0
Neighbor Chassis-Name          : HP-3800-24G-PoEP-2XG
Neighbor Chassis-Description   : HP J9587A 3800-24G-PoE+-2XG Switch, revision...
Neighbor Chassis-ID            : 10:60:4b:39:3e:80
Neighbor Management-Address    : 192.168.1.1
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge
Neighbor Port-ID               : 1/1/1
Neighbor Port-Desc             : 1/1/1
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
TTL                            : 120
```

Showing information for interface **1/3/10** when the neighbor sends a DOT3 power TLV:

```
switch# show lldp neighbor-info 1/3/10
Port                           : 1/3/10
Neighbor Entries               : 1
Neighbor Entries Deleted       : 0
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 0
Neighbor Chassis-Name          : 84:d4:7e:ce:5d:68
Neighbor Chassis-Description   : ArubaOS (MODEL: 325), Version HPE_ANW IAP
Neighbor Chassis-ID            : 84:d4:7e:ce:5d:68
Neighbor Management-Address    : 169.254.41.250
Chassis Capabilities Available : Bridge, WLAN
```

```
Chassis Capabilities Enabled   : WLAN
Neighbor Port-ID               : 84:d4:7e:ce:5d:68
Neighbor Port-Desc             : eth0
TTL                            : 120
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
Neighbor PoE information       : DOT3
Neighbor Power Type            : TYPE2 PD
Neighbor Power Priority        : Unkown
Neighbor Power Source          : Primary
PD Requested Power Value       : 25.0 W
PSE Allocated Power Value: 25.0 W
Neighbor Power Supported       : Yes
Neighbor Power Enabled         : Yes
Neighbor Power Class           : 5
Neighbor Power Paircontrol     : No
PSE Power Pairs                : Signal
```

Showing information for interface **1/1/1** when it has multiple neighbors (displays a maximum of four):

```
switch# show lldp neighbor-info 1/1/1

Port                           : 1/1/1
Neighbor Entries               : 4
Neighbor Entries Deleted       : 0
Neighbor Entries Dropped       : 0
Neighbor Entries Aged-Out      : 0
Neighbor Chassis-Name          : switch
Neighbor Chassis-Description   : hpe_anw JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID            : 1c:98:ec:fe:25:00
Neighbor Management-Address    : 10.1.1.2
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/1
Neighbor Port-Desc             : 1/1/1
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
TTL                            : 120
Neighbor Chassis-Name          : switch
Neighbor Chassis-Description   : hpe_anw JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID            : 1c:98:ec:fe:25:01
Neighbor Management-Address    : 10.1.1.3
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/1
Neighbor Port-Desc             : 1/1/1
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
TTL                            : 120
Neighbor Chassis-Name          : switch
Neighbor Chassis-Description   : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID            : 1c:98:ec:fe:25:02
Neighbor Management-Address    : 10.1.1.4
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/1
```

```
Neighbor Port-Desc             : 1/1/1
Neighbor Port VLAN ID          : 50
Neighbor Port VLAN Name        : VLAN_50
Neighbor Port MFS              : 1500
TTL                            : 120
Neighbor Chassis-Name          : switch
Neighbor Chassis-Description   : hpe_anw JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID            : 1c:98:ec:fe:25:03
Neighbor Management-Address    : 10.1.1.5
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/1
Neighbor Port-Desc             : 1/1/1
Neighbor Port VLAN ID          : 100
Neighbor Port VLAN Name        : VLAN_100
Neighbor Port MFS              : 1500
TTL                            : 120
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show lldp neighbor-info detail

```
show lldp neighbor-info detail [vsx-peer]
```

Description

Shows detailed LLDP neighbor information for all LLDP neighbor connected interfaces.

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

Examples

Showing detailed LLDP information for all interfaces:

```
switch# show lldp neighbor-info detail

LLDP Neighbor Information
=========================
```

```
Total Neighbor Entries          : 6
Total Neighbor Entries Deleted  : 2
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 2

--------------------------------------------------------------------------------

Port                            : 1/1/1
Neighbor Entries                : 1
Neighbor Entries Deleted        : 0
Neighbor Entries Dropped        : 0
Neighbor Entries Aged-Out       : 0
Neighbor Chassis-Name           : 6300
Neighbor Chassis-Description    : hpe_anw ...
Neighbor Chassis-ID             : 38:11:17:1a:d5:00
Neighbor Management-Address     : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled    : Bridge, Router
Neighbor Port-ID                : 1/1/4
Neighbor Port-Desc              : 1/1/4
Neighbor Port VLAN ID           : 1
Neighbor Port VLAN Name         : DEFAULT_VLAN_1
Neighbor Port MFS               : 1500
TTL                             : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported     : true
Neighbor Auto-Neg Enabled       : true
Neighbor Auto-Neg Advertised    : 1000 BASE_TFD, 100 BASE_T4, 10 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    : hpe_anw...
Neighbor Chassis-ID             : 38:11:17:1a:d5:00
Neighbor Management-Address     : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled    : Bridge, Router
Neighbor Port-ID                : 1/1/5
Neighbor Port-Desc              : 1/1/5
Neighbor Port VLAN ID           : 1
Neighbor Port VLAN Name         : DEFAULT_VLAN_1
Neighbor Port MFS               : 1500
TTL                             : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported     : true
Neighbor Auto-Neg Enabled       : true
Neighbor Auto-Neg Advertised    : 1000 BASE_TFD, 100 BASE_T4, 10 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   : hpe_anw ...
Neighbor Chassis-ID            : 38:11:17:1a:d5:00
Neighbor Management-Address    : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/6
Neighbor Port-Desc             : 1/1/6
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
TTL                            : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported    : true
Neighbor Auto-Neg Enabled      : true
Neighbor Auto-Neg Advertised   : 1000 BASE_TFD, 100 BASE_T4, 10 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   : hpe_anw ...
Neighbor Chassis-ID            : 38:11:17:1a:d5:00
Neighbor Management-Address    : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID               : 1/1/19
Neighbor Port-Desc             : 1/1/19
Neighbor Port VLAN ID          : 1
Neighbor Port VLAN Name        : DEFAULT_VLAN_1
Neighbor Port MFS              : 1500
TTL                            : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported    : true
Neighbor Auto-Neg Enabled      : true
Neighbor Auto-Neg Advertised   : 1000 BASE_TFD, 100 BASE_T4, 10 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   : hpe_anw ...
Neighbor Chassis-ID            : 38:11:17:1a:d5:00
Neighbor Management-Address    : 38:11:17:1a:d5:00
Chassis Cap
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show lldp neighbor-info mgmt

```
show lldp neighbor-info mgmt
```

Description

Displays information about neighboring devices connected to the OOBM interface.

Examples

Showing LLDP information for the OOBM interface:

```
switch# show lldp neighbor-info mgmt

Port                            : mgmt
Neighbor Entries                : 1
Neighbor Entries Deleted        : 0
Neighbor Entries Dropped        : 0
Neighbor Entries Aged-Out       : 0
Neighbor Chassis-Name           : HP-3800-24G-PoEP-2XG
Neighbor Chassis-Description    : HP J9587A 3800-24G-PoE+-2XG Switch, revision...
Neighbor Chassis-ID             : 10:60:4b:39:3e:80
Neighbor Management-Address     : 192.168.1.1
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled    : Bridge
Neighbor Port-ID                : mgmt
Neighbor Port-Desc              : mgmt
TTL                             : 120
```

Showing LLDP information for the OOBM interface when there are four neighbors:

```
switch# show lldp neighbor-info mgmt

Port                            : mgmt
Neighbor Entries                : 4
Neighbor Entries Deleted        : 0
Neighbor Entries Dropped        : 0
Neighbor Entries Aged-Out       : 0
Neighbor Chassis-Name           : switch
Neighbor Chassis-Description    : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID             : 1c:98:ec:fe:25:00
Neighbor Management-Address     : 10.1.1.2
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled    : Bridge, Router
Neighbor Port-ID                : 1/1/1
Neighbor Port-Desc              : 1/1/1
```

```
TTL                             : 120

Neighbor Chassis-Name           : switch
Neighbor Chassis-Description    : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID             : 1c:98:ec:fe:25:01
Neighbor Management-Address     : 10.1.1.3
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID                : 1/1/1
Neighbor Port-Desc              : 1/1/1
TTL                             : 120

Neighbor Chassis-Name           : switch
Neighbor Chassis-Description    : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID             : 1c:98:ec:fe:25:02
Neighbor Management-Address     : 10.1.1.4
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID                : 1/1/1
Neighbor Port-Desc              : 1/1/1
TTL                             : 120

Neighbor Chassis-Name           : switch
Neighbor Chassis-Description    : HPE ANW JL375A 8400X XL.01.01.0001
Neighbor Chassis-ID             : 1c:98:ec:fe:25:03
Neighbor Management-Address     : 10.1.1.5
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID                : 1/1/1
Neighbor Port-Desc              : 1/1/1
TTL                             : 120
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp statistics

`show lldp statistics [<INTERFACE-ID>][vsx-peer]`

Description

Shows global LLDP statistics or statistics for a specific interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: **member/slot/port**.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing global statistics for all interfaces:

```
switch# show lldp statistics
LLDP Global Statistics
======================

Total Packets Transmitted            : 19
Total Packets Received               : 19
Total Packets Received And Discarded : 0
Total TLVs Unrecognized              : 0

LLDP Port Statistics
====================

PORT-ID        TX-PACKETS     RX-PACKETS     RX-DISCARDED   TLVS-UNKNOWN
-------------------------------------------------------------------------
1/1/1          7              7              0              0
1/1/2          7              7              0              0
1/1/3          0              0              0              0
1/1/4          0              0              0              0
1/1/5          0              0              0              0
...
mgmt           5              5              0              0

```
```

Showing statistics for interface **1/1/1**:

```
switch# show lldp statistics 1/1/1

LLDP Statistics
===============

Port Name                          : 1/1/1
Packets Transmitted                : 159
Packets Received                   : 163
Packets Received And Discarded     : 0
Packets Received And Unrecognized : 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information
```

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

show lldp statistics mgmt

```
show lldp statistics mgmt
```

Description

Shows LLDP statistics for the OOBM interface.

Example

Showing LLDP statistics for the OOBM interface:

```
switch# show lldp statistics mgmt

LLDP Statistics
===============

Port Name                          : mgmt
Packets Transmitted                : 20
Packets Received                   : 23
Packets Received And Discarded     : 0
Packets Received And Unrecognized  : 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp tlv

```
show lldp tlv[vsx-peer]
```

Description

Shows the LLDP TLVs that are configured for send and receive.

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

Example

```
switch# show lldp tlv

TLVs Advertised
===============

Management Address
Port Description
Port VLAN-ID
System Capabilities
System Description
System Name
VLAN Name
MFS
OUI
```

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.

Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP) is a proprietary layer 2 protocol supported by most Cisco devices. It is used to exchange information, such as software version, device capabilities, and voice VLAN information, between directly connected devices, such as a VoIP phone and a switch.

CDP support

By default, CDP is enabled on each active switch port. This is a read-only capability, which means the switch can receive and store information about adjacent CDP devices, but does not generate CDP packets (except when communicating with Cisco IP phones.)

The switch supports CDPv2 only and does not support SNMP MIB traps.

When a CDP-enabled port receives a CDP packet from another CDP device, it enters data for that device into the CDP Neighbors table, along with the port number on which the data was received. It does not forward the packet. The switch also periodically purges the table of any entries that have expired. (The

holdtime for any data entry in the switch CDP Neighbors table is configured in the device transmitting the CDP packet and cannot be controlled in the switch receiving the packet.) A switch reviews the list of CDP neighbor entries every three seconds and purges any expired entries.

Support for legacy Cisco IP phones

Autoconfiguration of legacy Cisco IP phones for tagged voice VLAN support requires CDPv2.

On initial boot-up, and sometimes periodically, a Cisco phone queries the switch and advertises information about itself using CDPv2. When the switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone, the switch immediately responds with the voice VLAN ID in a reply packet using the VoIP VLAN Reply TLV (type 0x0e). This enables the Cisco phone to boot properly and send traffic on the advertised voice VLAN ID.

The switch CDP packet includes these TLVs:

- CDP Version: 2
- CDP TTL: 180 seconds
- Checksum
- Capabilities (type 0x04): 0x0008 (is a switch)
- Native VLAN: The PVID of the port
- VoIP VLAN Reply (type 0xe): voice VLAN ID (same as advertised by LLDP-MED)
- Trust Bitmap (type 0x12): 0x00
- Untrusted port CoS (type 0x13): 0x00

CDP commands

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
```

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
```

Command History

Release	Modification
10.07 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
```

Command History

Release	Modification
10.07 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
```

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       HPE_ANW-3810M-24G-1-slot... HPE ANW Sw               S
```

Showing CDP information for interface **1/1/1**:

```
switch(config)# show cdp neighbor-info 1/1/1
Local Port         : 1/1/1
MAC                : 70:10:6f:86:78:7f
Device ID          : HPE_ANW-3810M-24G-1-slot(70106f-867800)
Address            : 127.0.0.1
Platform           : HPE ANW Sw
Duplex             : half
Version            : Revision KB.16.07.0002, ROM KB.16.01....
Capability         : switch
Native VLAN        : 1
Voice VLAN Support : No
Neighbor Port-ID   : 1
```

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
```

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
```

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.

Chapter 17
Zero Touch Provisioning

Zero Touch Provisioning (ZTP) enables the auto-configuration of factory default switches without a network administrator onsite.

When a switch is booted from its factory default configuration, ZTP autoprovisions the switch by automatically downloading and installing a firmware file, a configuration file, or both. With ZTP, even a nontechnical user (for example: a store manager in a retail chain or a teacher in a school) can deploy devices at a site.

ZTP connection priorities

An HPE Aruba Networking CX switch supports ZTP provisioning on an Out-of-Band Management (OOBM) port, a data port (vlan 1), or an image and config file provided via USB.

Priority is given to ZTP options received on the OOBM port. If the switch receives ZTP configuration options on a data port first or from a DHCPv6 server connected to an OOBM port, the switch waits for an additional 30 seconds to see if higher-priority ZTP options will be received on an OOBM port also.

Priority is given to ZTPv4 options over ZTPv6 options, so connection priorities are as follows, from highest to lowest priority:

1. ZTP options received via USB.
2. ZTP options received from a DHCPv4 server on an OOBM port.
3. ZTP options received from a DHCPv4 server on a data port.
4. ZTP options received from a DHCPv6 server on an OOBM port.

ZTP support

The switch supports standards-based Zero Touch Provisioning (ZTP) operations as follows:

- ZTP operations are supported over IPv4 and IPv6 connections.
- The switch must be running the factory default configuration.
- The switch can connect to the DHCP server from the OOBM management port.
- The configuration file is a text file or JSON file that becomes the startup and running configuration on the switch after the ZTP operation is complete. The configuration can be in CLI or in JSON format.
- When the switch is started using the factory default configuration, the ZTP operation is started automatically and is active until any running configuration of the switch is modified. There is no CLI command required to start the operation.
- You must configure the DHCP server to provide a standards-based ZTP server solution. Options and features that are specific to Network Management Solution (NMS) tools, such as AirWave, are not supported.
  - Aruba Central on-premise can manage AOS-CX switches on supported models through DHCP ZTP using two approaches:
    - On the DHCP server, configure DHCP option-60 as "ArubaInstantAP" 90 and provide the value in option-43 in the format *<group-details>, <aruba-central-on-prem-ip-or-fqdn>, <shared-token>.*

- On the DHCP server, configure DHCP option-60 as HPE vendor VCI and provide the value in option-43 in the tag-length-value (TLV) format. Next, enter the Aruba Central on-premise fully qualified domain name (FQDN) or IPv4 address as the value for sub-option code 146 using the format: *<group-details>, <aruba-central-on-prem-ip-or-fqdn>, <shared-token>*.

Supported ZTP options from a DHCPv4 server are:

DHCP option	Description
43	Vendor Specific Information
43 suboption 144	Name of the configuration file
43 suboption 145	Name of the firmware image file
43 suboption 146	FQDN or IPv4 address of the Aruba Central on-premise server
43 suboption 148	FQDN or IPv4 or IPv6 address of the HTTP Proxy
60	Vendor Class Identifier (VCI)
66	IPv4 or IPv6 address of the TFTP or HTTP server (Specifying a host name instead of an IP address is not supported.)
67	Name of the configuration file (Option 43 suboption 144 takes precedence over this option.)

Unique ZTP IPv6 options can be sent from the DHCPv6 Server based on MAC address of the switch or based on the DHCP Vendor class Identifier of the switch. Supported ZTP options from a DHCPv6 server are:

DHCP option	Description
59	IPv6 address of the TFTP/HTTP server. The image file name also can be given in this URL or in the VCA option-17. **NOTE:** the boot file URL will support TFTPv6 Server or HTTP Server option with IPv6 address or FQDN name.
17 suboption 145	Name of the image file.
17 suboption 144	Name of the configuration file.

The switch supports the following standards:

- RFC 2131, *Dynamic Host Configuration Protocol*.
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*. Support is limited to the options listed in the table "Supported DHCP options for ZTP on AOS-CX."
- RFC 5970, *DHCPv6 Options for Network Boot*. Support is limited to the options listed in the table "Supported DHCP options for ZTP on AOS-CX."

Hewlett Packard Enterprise recommends that you implement ZTP in a secure and private environment. Any public access can compromise the security of the switch, as follows:

- ZTP is enabled only in the factory default configuration of the switch, DHCP snooping is not enabled. The Rogue DHCP server must be manually managed.
- The DHCP offer is in plain data without encryption.

Setting up ZTP on a trusted network

The following procedure is an overview of setting up a Zero Touch Provisioning (ZTP) environment to provision newly installed switches automatically. The procedure is intended for network administrators who are familiar with automatically provisioning switches in a network, and does not provide detailed information about configuring or managing switches.

Procedure

1. For each switch model to be provisioned using ZTP, do the following:
   a. Obtain the switch firmware image file.
   b. Prepare the switch configuration file. The configuration file becomes the running configuration and the startup configuration on the switch.
2. Set up a TFTP or HTTP server and record its IPv4 or IPv6 address. The address is required when you set up the DHCP server. The switch must be able to reach the TFTP or HTTP server and DHCP server, either on the same subnet, or on a remote subnet via DHCP relay.

   For switches that do not support ZTP connections through a data port, use the management port and management network.
3. Publish the configuration files and image files to the TFTP or HTTP server. You need to know the locations of the files and the IPv4/IPv6 address of theTFTP or HTTP server when you set up the vendor class options on the DHCP server.
4. On the DHCP server, set up vendor classes for each switch model you plan to provision. To do this you need the following information:
   - The IPv4/IPv6 address of the TFTP or HTTP server. Using a host name is not supported.
   - The path to the switch configuration and firmware image files on the TFTP or HTTP server.
   - The vendor class identifier (VCI) for each switch model.

   You can obtain the VCI by entering the **show dhcp client vendor-class-identifier** command from a switch CLI command prompt in the manager context. The VCI is the text string in the response that starts with **Aruba**.

   For example:

   ```
   switch# show dhcp client vendor-class-identifier
   Vendor Class Identifier: Aruba xxxxx xxxx
   ```

   Where x indicates the switch model number.
5. At the installation site, provide the switch installer with a Cat6 network cable connected to the network that includes the DHCP and TFTP or HTTP servers, and information about the switch port to use. The switch installer plugs the cable into the data port you specify.

   The ZTP operation begins when power is applied to the switch after the network cable is installed.
6. Assuming the downloaded configuration includes a way to access the CLI of the switch, you can enter the following command to show the options offered by the DHCP server and the status of the ZTP operation:

   ```
   show ztp information
   ```

ZTP using USB

AOS-CX supports EXT4, FAT-16, and FAT-32 USB file systems for ZTP. To perform zero-touch provisioning via USB, the image and config files should be in one of the following folders on the USB device.

The file with extension .**swi** is recognized as an image file and the file with extension .**cfg** is recognized as a configuration file. These file extensions are case sensitive.

A serial-number specific folder:

- AOSCX/CNXXXXXXXX/ZTP/<image.swi>
- AOSCX/CNXXXXXXXX/ZTP/<config.cfg>

A vendor-class specific folder:

- AOSCX/PRODUCTNAME_PARTNUM/ZTP/<image.swi>
- AOSCX/PRODUCTNAME_PARTNUM/ZTP/<config.cfg>
  (for example: AOSCX/8320_JL479A/ZTP)

A generic configuration folder:

- AOSCX/ZTP/<image.swi>
- AOSCX/ZTP/<config.cfg>

If multiple paths are present, then the priority is given in the following order:

1. The serial number specific folder with an image file or configuration file.
2. The vendor class specific folder with an image file or configuration file.
3. The generic configuration folder with an image file or configuration file.

You can identify the switch product name and part number you should use to create a ZTP folder by issuing the command **show dhcp client vendor-class-identifier**. For example:

```
switch# show dhcp client vendor-class-identifier
Vendor Class Identifier:  Aruba <xxxx> <yyyy>
```

Where **<xxxx>** is the part number and **<yyyy>** is the product name in the output of this command.

If multiple image or configuration files are present in these ZTP folders, the first file that shows up in the output of the **ls -1 <usb_ztp_path**> command will be used for ZTP provisioning

If the switch boots up with a factory default configuration and a USB device is connected to the switch, the switch looks for the presence of ZTP-related folders. The switch then will be provisioned with the image and configuration files provided via USB. If either an image or a configuration file is present in the ZTP related folders on USB, then the switch will be provisioned with the respective file provided from the USB device.

ZTP using USB will not be triggered and the switch will continue with ZTP using DHCP in the following scenarios:

- There is no USB device connected.
- The USB device does not have the ZTP-specific folder.

- The ZTP folder has no image or configuration files in the first 127 files listed in the folder.
- The USB drive containing ZTP specific files is inserted into the device after it has booted up. (A device reboot is required to initiate the ZTP process using the USB.)

To confirm that the ZTP process has been triggered, issue the command **show ztp information**.

Performing an upgrade from a USB device without ZTP

To perform a manual upgrade using an image and configuration file from a USB device, issue the following copy commands to download the image and config file from the USB device directly on to the switch.

```
copy usb:/file <running-config|startup-config|primary|secondary
```

ZTP process during switch boot

1. The switch boots up with the factory default configuration.

   If the ZTP operation detects that the switch configuration is different from the factory default configuration, the ZTP operation ends. The switch must be configured at the installation site.
2. The switch sends out a DHCP discovery from the management port.

   The switch waits to receive DHCP options indefinitely or until the running configuration is modified. If a DHCP IP address is received but no DHCP options are received, the switch waits an additional minute before ending the ZTP operation.

   After the ZTP operation ends, there is no automatic retry. You can either attempt to boot the switch with the factory default configuration again, configure the switch at the installation site, or use the ZTP force-provision CLI to trigger the ZTP process, ignoring the present running configuration of the switch.
   - Once force-provision is enabled, new DHCP requests are sent from the switch. Disabling force-provision does not stop the DHCP already in progress, but only changes the switch configuration status of force-provision.
   - If ZTP fails while force-provision is enabled, there is no automatic retry. To retry, **ztp force-provision** should be disabled and re-enabled to clear the current ZTP state and send a new DHCP request. When **ztp force-provision** is already enabled on the switch, re-enabling it results in no operation.
   - If the DHCP server is configured to provide both ZTP image and configuration options and there is a non-default startup configuration present on the switch, clearing the non-default startup configuration before triggering **ztp force-provision** is recommended. If an image is downloaded via ZTP, the switch reboots once the image download is complete and ZTP force-provision configuration is lost, causing ZTP to enter into a failed state. ZTP force-provision will need to be enabled again to continue the process.
3. The DHCP server responds with an offer containing the following:
   - The IPv4 or IPv6 address of the TFTP or HTTP server
   - One or both of the following:
     - The name of the firmware image file
     - The name of the configuration file
   - Aruba Central Location (optional) including the shared token value for the on-premise server
   - HTTP Proxy Location (optional)

4. If a firmware image file is offered, the ZTP operation downloads the image file from the TFTP or HTTP server to the switch. If the current switch image and downloaded firmware image version do not match, then the switch boots with the downloaded image:
   - If the image upgrade fails, the switch retains its original firmware image and the ZTP operation ends with a failed status.
   - If the image upgrade succeeds, the ZTP operation is started again after the switch reboots. Because the downloaded image file matches the image file installed on the switch, the ZTP operation continues, and checks if a configuration file is offered.
5. If a configuration file is offered, the ZTP operation downloads the configuration file copies the file to the running-config and then to the startup-config of the switch:
   - If the startup configuration update fails, the switch retains its factory-default running configuration and the ZTP operation ends with a failed status.
     - If the copy operation fails, the ZTP operation ends with a failed status.
     - If the copy operation succeeds, the ZTP operation ends successfully.

ZTP VSF switchover support

ZTP status is not synced in the VSF stack. When the VSF stack is formed, configuration changes are applied on the conductor switch, which is then synced to standby switch. When the switchover is performed on the VSF stack, the standby becomes the new conductor switch.

As part of the switchover process, the ZTP daemon starts on the new conductor. The status of the ZTP is failed because there are configuration changes present.

ZTP commands

show ztp information

```
show ztp information
```

Description

Shows information about Zero Touch Provisioning (ZTP) operations performed on the switch.

Usage

When a switch configured to use ZTP is booted from a factory default configuration, the switch contacts a DHCP server, which offers options for obtaining files used to provision the switch:

- The IPv4/IPv6 address of TFTP Server or the IPv6 address of HTTP server
- The name of the image file
- The name of the configuration file
- The HPE Aruba Networking Central FDQN or IPv4/IPv6 address
- The HTTP proxy FDQN or IPv4/IPv6 address

The **show ztp information** command shows the options offered by the DHCP server and the status of the ZTP operation.

The status of the ZTP operation is one of the following:

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/HTTP 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 or IPv6 address but no ZTP options were received within 1 minute or ZTP force-provision is triggered and no ZTP options are received within 3 minutes.
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).
Failed - HTTP server unreachable	The HTTP server is not reachable at the specified IP address
Failed - Invalid configuration file from USB	The configuration file is invalid or it is not in the proper format.
Failed - Invalid image file from USB	The image file is invalid or it is not in the proper format.
Failed - Error while copying	ZTP failed to copy the configuration file from the USB device due to a file permissions, file access or system error (for example, if the switch is out of memory), if the user interrupts

the configuration from USB	the ZTP process, or if the fille is deleted from the USB device. This message may also display in the event of an unknown error.
Failed - Error while copying the image from USB	ZTP failed to copy the image file from the USB device due to a file permissions, file access or system error (for example, if the switch is out of memory), if the user interrupts the ZTP process, or if the fille is deleted from the USB device. This message may also display in the event of an unknown error.

In the case of reconnection, connect with a main or alternative location to the COP instance as a user. The current connection is shown in the **Central location** field.
Scenario 1: If the location the device is currently connected on is updated, the system reconnects in order to connect with the new location.
Scenario 2: If the location in which the device is not currently connected on is updated, the DUT does not go through the reconnection process.

Examples

Showing switch image and config download from an IPv4 TFTP server in progress after receiving ZTP options:

```
switch# show ztp information
TFTP Server                                    : 10.0.0.2
Image File                                     : TL_10_02_0001.swi
Configuration File                             : ztp.cfg
ZTP Status                                     : In-progress - Image download and verification
HPE ANW Central Location                       : NA
Alternative HPE ANW Central Location            : NA
HPE ANW Central Shared Token                   : NA
Force-Provision                                : Enabled
HTTP Proxy Location                            : NA
```

Showing switch image download failure from an IPv4 TFTP server because the server was unreachable

```
switch# show ztp information
TFTP Server                                    : 10.0.0.2
Image File                                     : TL_10_02_0001.swi
Configuration File                             : ztpv6.cfg
ZTP Status                                     : Failed - TFTP server unreachable
HPE ANW Central Location                       : NA
Alternative HPE ANW Central Location            : NA
HPE ANW Central Shared Token                   : NA
Force-Provision                                : Enabled
HTTP Proxy Location                            : NA
```

Showing a successful switch configuration download from an IPv6 HTTP server

```
switch# show ztp information
HTTP Server                                     : http://[2001::50]
Image File                                     : TL_10_15_0001.swi
Configuration File                             : config_file
ZTP Status                                     : Success
HPE ANW Central Location                       : NA
Alternative HPE ANW Central Location            : NA
```

```
HPE ANW Central Shared Token                      : NA
Force-Provision                                   : Enabled
HTTP Proxy Location                               : NA
```

The switch received image and configuration files from a serial-number specific folder on a USB device, and ZTP was successful.

```
switch# show ztp information
TFTP Server                           : NA
Image File                            : usb:/AOSCX/TW88KHD005/GL_10_16_00001.swi
Configuration File                    : usb:/AOSCX/TW88KHD005/ztp.cfg
Status                                : Success
HPE ANW Central Location              : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token          : NA
Force-Provision                       : Disabled
HTTP Proxy Location                   : NA
```

The switch received image and configuration files from a generic folder on a USB device, and ZTP was successful.

```
switch# show ztp information
TFTP Server                           : NA
Image File                            : usb:/AOSCX/ztp/ML_10_15_1000F.swi
Configuration File                    : usb:/AOSCX/ztp/config.cfg
Status                                : Success
HPE ANW Central Location              : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token          : NA
Force-Provision                       : Disabled
HTTP Proxy Location                   : NA
```

The switch received an image file from a vendor-class specific folder on a USB device, and ZTP was successful.

```
switch# show ztp information
TFTP Server                           : NA
Image File                            : usb:/AOSCX/8325_JL636A/GL_10_16_1000A.swi
Configuration File                    : NA
Status                                : Success
HPE ANW Central Location              : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token          : NA
Force-Provision                       : Disabled
HTTP Proxy Location                   : NA
```

Command History

Release	Modification
10.16	The output of this command can show the status of ZTP over USB.
10.07 or earlier	--

Command Information

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

ztp force provision

```
ztp force-provision
no ztp force-provision
```

Description

Starts on-demand ZTP via DHCP.

Usage

DHCP options received are processed independent of the current state of configuration on the switch. Previous ZTP options are cleared, such as the ZTP TFTP server, image file, configuration file, HPE Aruba Networking Central location, and HTTP proxy location, and the switch sends a DHCP request. ZTP using USB is not triggered by this command.

Examples

In the following example, force-provision is enabled.

```
switch# configure terminal
switch(config)# ztp force-provision
```

In the following example, force-provision status is checked while enabled.

```
switch# show ztp information
TFTP Server                                 : 10.0.0.2
Image File                                  : TL_10_02_0001.swi
Configuration File                          : ztp.cfg
Status                                      : Success
HPE ANW Central Location                    : NA
HPE ANW Central Shared Token                : NA
Force-Provision                             : Enabled
HTTP Proxy Location                         : NA
```

In the following example, force-provision is disabled.

```
switch# configure terminal
switch(config)# no ztp force-provision
```

In the following example, force-provision status is checked while disabled.

```
switch# show ztp information
TFTP Server                                 : 10.0.0.2
Image File                                  : TL_10_02_0001.swi
Configuration File                          : ztp.cfg
Status                                      : Success
HPE ANW Central Location                    : NA
HPE ANW Central Shared Token                : NA
```

```
Force-Provision                                 : Disabled
HTTP Proxy Location                             : NA
```

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.

Thermal Management

Thermal management consists of the **fand** and **tempd** daemons, that manage the fans and temperature sensors for the system respectively. They are responsible for monitoring temperatures, adjusting fan speeds to keep the system at nominal temperatures, initiating shutdown sequences for chassis, subsystems, or transceivers during over-temperature conditions, and reporting temperatures, sensor states, fan speeds, and fan states.

Thermal management support

	Description	Platforms
Transceiver Thermal Management	When the transceiver thermal management capability is enabled, a temperature sensor will be available for each transceiver that supports thermal monitoring.	8325H 9300-32C8D 9300-32D
Thermal Shutdown Behavior	Thermal shutdown is a critical safety mechanism designed to prevent hardware damage caused by overheating. When critical temperature thresholds are exceeded, thermal daemons log an event and initiate a shutdown sequence to power down the affected components gracefully.	All platforms
Chassis (Switch) Thermal Shutdown	If a temperature sensor exceeds its critical threshold and the associated subsystem does not support being powered off, the entire chassis will shut down for a five minute cool down period. If the critical temperature is detected again after reboot, the shutdown sequence will repeat.	All platforms
Subsystem (Line Card, Fabric Card) Thermal Shutdown	If a temperature sensor exceeds its critical threshold and the associated subsystem supports being powered off, that subsystem will shut down for a five minute cool	5420 6400 8400

	Description	Platforms
	down period. If the critical temperature is detected again after reboot, the shutdown sequence will repeat.	
Transceiver Thermal Shutdown	If a transceiver's temperature sensor exceeds its critical threshold and the transceiver is configured to shut down upon exceeding the critical threshold, it will power down for a five-minute cool down period. If the critical temperature is detected again after reboot, the shutdown sequence will repeat.	8325H 9300-32C8D 9300-32D

Transceiver Thermal Management

Transceiver temperature sensors are visible on REST API calls, SNMP and CLI (show environment temperature). Events logs also are triggered upon thermal status changes, shutdown and recovery. If a transceiver exceeds the temperature threshold and it is hot swapped, the cool time timer is canceled and the transceiver is re-enabled. There is no limit to the number of times a transceiver is thermally disabled and re-enabled if it's continuously above the critical temperature threshold.

This is an example of the temperature information on the normal conditions.

```
switch# show environment temperature
Temperature information
-------------------------------------------------------------------------------
                                                  Current
Mbr/Slot-Sensor                 Module Type      temperature  Status
-------------------------------------------------------------------------------
1/1-xcv-5                       line-card-module     66.45 C    normal
...
```

If the temperature raises to 70 degrees Celsius, the status changes to **overtemp**.

```
switch# show environment temperature
Temperature information
-------------------------------------------------------------------------------
                                                  Current
Mbr/Slot-Sensor                 Module Type      temperature  Status
-------------------------------------------------------------------------------
1/1-xcv-5                       line-card-module     70.00 C    overtemp
...
```

The status change will generate this event log: **Temperature sensor 1/1-xcv-5 status is overtemp at 70.000000 degC**

If the temperature raises to 82 degrees Celsius, for example, the status changes to **emergency**. The transceiver is disabled and the cool own period begins. The status change and the disabling of the interface reflect in the event logs.

```
Temperature sensor 1/1-xcv-5 status is overtemp at 70.000000 degC
Temperature sensor 1/1-xcv-5 status is critical at 82.000000 degC
Disabling interface 1/1/5 transceiver for 5 minutes - temperature sensor 1/1-xcv-5
status is emergency at 82.000000 degC
```

This is an example of the **show interface** command when the interface is **disabled:**

```
switch# show int 1/1/5
Interface 1/1/5 is down
Admin state is down
State information: Transceiver disabled - Module disabled by system thermal
management
Link state: down for 1 hour (since Wed May 14:22:17:42 UTC 2025)
Link transitions: 0
Description:
Persona:
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 1500
Type 40G-eSR4 / QSPF+ eSR4
Full-duplex
qos trust none
Speed 0 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
L3 Counters: Rx Desabled, Tx Disabled
Rate collection interval: 300 seconds

Rates                            RX                   TX        Total (RX+TX)
------------ -------------------- -------------------- --------------------
Mbits / sec                  0.00                 0.00                 0.00
KPkts / sec                  0.00                 0.00                 0.00
  Unicast                    0.00                 0.00                 0.00
  Multicast                  0.00                 0.00                 0.00
  Broadcast                  0.00                 0.00                 0.00
Utilization %                0.00                 0.00                 0.00

Statistics                       RX                   TX                Total
------------ -------------------- -------------------- --------------------
Packets                         0                    0                    0
  Unicast                       0                    0                    0
  Multicast                     0                    0                    0
  Broadcast                     0                    0                    0
Bytes                           0                    0                    0
Jumbos                          0                    0                    0
Dropped                         0                    0                    0
Filtered                        0                    0                    0
Pause Frames                    0                    0                    0
L3 Packets                      0                    0                    0
L3 Bytes                        0                    0                    0
Errors                          0                    0                    0
  CRC/FCS                       0                  n/a                    0
  Collision                   n/a                    0                    0
  Runts                         0                  n/a                    0
  Giants                        0                  n/a                    0
Other                           0                    0                    0
```

Once the cool down period is over, the transceiver is enabled. Therefore, the status changes to normal and the corresponding event log is triggered:

```
Temperature sensor 1/1-xcv-5 status is overtemp at 70.000000 degC
Temperature sensor 1/1-xcv-5 status is critical at 82.000000 degC
Disabling interface 1/1/5 transceiver for 5 minutes - temperature sensor 1/1-xcv-5
status is emergency at 82.000000 degC
Enabling interface 1/1/5 transceiver - thermal disablement period has expired
```

If the transceiver is hot swapped, the interface is re-enabled and the event logs are:

```
Temperature sensor 1/1-xcv-5 status is overtemp at 70.000000 degC
Temperature sensor 1/1-xcv-5 status is critical at 82.000000 degC
Disabling interface 1/1/5 transceiver for 5 minutes - temperature sensor 1/1-xcv-5
status is emergency at 82.000000 degC
Enabling interface 1/1/5 transceiver - thermal disablement cancelled due to hot-
swap of transceiver
```

The examples above apply to the 9300-32D Switch Series. The output of these commands may vary in other platforms. The temperature thresholds shown here are for illustration purposes only.

allow-non-failsafe-updates

```
allow-non-failsafe-updates <num_minutes>
```

Description

Allow non-failsafe updates of programmable devices for the specified number of minutes, or **enter** 0 to disallow unsafe updates. The maximum permitted value is 120 minutes.

Example

The following example will enable non-failsafe updates of programmable devices for the next 30 minutes.

```
switch(config)#  allow-non-failsafe-updates 30

This command will enable non-failsafe updates of programmable devices for
the next 30 minutes.  You will first need to wait for all line and fabric
modules to reach the ready state, and then reboot the switch to begin applying any
needed
updates.  Ensure that the switch will not lose power, be rebooted again, or have
any
modules removed until all updates have finished and all line and fabric modules
have
returned to the ready state

WARNING: Interrupting these updates may make the product unusable!

Continue [y/n] ? y

Unsafe updates      : allowed (less than 30 minute(s) remaining)
```

Command History

Release	Modification
10.15.1010	--

Command Information

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

bluetooth disable

```
bluetooth disable
no bluetooth disable
```

Description

Disables the Bluetooth feature on the switch. The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE). Bluetooth is enabled by default.

The **no** form of this command enables the Bluetooth feature on the switch.

Example

Disabling Bluetooth on the switch. <*XXXX*> is the switch platform and <*NNNNNNNNNN*> is the device identifier.

```
switch(config)# bluetooth disable
switch# show bluetooth
Enabled              : No
Device name          : <XXXX>-<NNNNNNNNNN>

switch(config)# show running-config
...
bluetooth disabled
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	config	Administrators or local user group members with execution rights for this command.

bluetooth enable

```
bluetooth enable
no bluetooth enable
```

Description

This command enables the Bluetooth feature on the switch. The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE).

Default: Bluetooth is enabled by default.

The **no** form of this command disables the Bluetooth feature on the switch.

Usage

The default configuration of the Bluetooth feature is `enabled`. The output of the `show running-config` command includes Bluetooth information only if the Bluetooth feature is disabled.

The Bluetooth feature includes both Bluetooth Classic and Bluetooth Low Energy (BLE).

The Bluetooth feature requires the USB feature to be enabled. If the USB feature has been disabled, you must enable the USB feature before you can enable the Bluetooth feature.

Examples

```
switch(config)# bluetooth enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	`config`	Administrators or local user group members with execution rights for this command.

clear events

`clear events`

Description

Clears up event logs. Using the `show events` command will only display the logs generated after the `clear events` command.

Examples

Clearing all generated event logs:

```
switch# show events
-------------------------------------------------
show event logs
-------------------------------------------------
2018-10-14:06:57:53.534384|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource
utilization poll interval is changed to 27
2018-10-14:06:58:30.805504|lldpd|103|LOG_INFO|MSTR|1|Configured LLDP tx-timer to
36
2018-10-14:07:01:01.577564|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource
```

```
utilization poll interval is changed to 49

switch# clear events

switch# show events
-------------------------------------------------
show event logs
-------------------------------------------------
2018-10-14:07:03:05.637544|hpe-sysmond|6301|LOG_INFO|MSTR|1|System resource
utilization poll interval is changed to 34
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

clear ip errors

`clear ip errors`

Description

Clears all IP error statistics.

Example

Clearing and showing ip errors:

```
switch# clear ip errors
switch# show ip errors
---------------------------------
Drop reason                Packets
---------------------------------
Malformed packets                0
IP address errors                0
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	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
```

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)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

hostname

```
hostname <HOSTNAME>
no hostname [<HOSTNAME>]
```

Description

Sets the host name of the switch.

The **no** form of this command 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)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

led locator

```
led locator
   on
   off
   flashing
   slow_blink
   fast_blink
   half_bright
```

```
no...
```

Description

Sets the state of the locator LED.

Parameter	Description
`on`	Turns on the LED.
`off`	Turns off the LED, which is the default value.
`flashing`	Sets the LED to blink on and off repeatedly.
`slow_blink`	Sets the LED to slow blink on and off.
`fast_blink`	Sets the LED to fast blink on and off.
`half_bright`	Sets the LED intensity to half bright.
`no`	Negates any configured parameter

Example

Setting the state of the locator LED:

```
switch# led locator flashing
```

Command History

Release	Modification
10.13	Starting with AOS-CX 10.13, this command will not take effect when it is sent to the switch from HPE Aruba Networking Central.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

mtrace

```
mtrace <IPV4-SRC-ADDR> <IPV4-GROUP-ADDR> [lhr <IPV4-LHR-ADDR>] [ttl <HOPS>]
   [vrf <VRF-NAME>]
```

Description

Traces the specified IPv4 source and group addresses.

Parameter	Description
IPV4-SRC-ADDR	Specifies the source IPv4 address to trace.
IPV4-GROUP-ADDR	Specifies the group IPv4 address to trace.
lhr *<IPV4-LHR-ADDR>*	Specifies the last hop router address from which to start the trace.
ttl *<HOPS>*	Specifies the Time-To-Live duration in hops. Range: 1 to 255 hops. Default: 8 hops.
vrf *<VRF-NAME>*	Specifies the name of the VRF. If a name is not specified the default VRF will be used.

Examples

Tracing with source, group, and LHR addresses and TTL:

```
(switch)# mtrace 20.0.0.1 239.1.1.1 lhr 10.1.1.1 ttl 10

Type escape sequence to abort.
Mtrace from 10.0.0.1 for Source 20.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0  10.0.0.1
-1  30.0.0.1 PIM  0 ms
-2  40.0.0.1 PIM  2 ms
-3  50.0.0.1 PIM  100 ms
-4  60.0.0.1 PIM  156 ms
-5  20.0.0.1 PIM  123 ms
```

Tracing with source and group addresses:

```
(switch)# mtrace 200.0.0.1 239.1.1.1

Type escape sequence to abort.
Mtrace from self for Source 200.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0  10.0.0.1
-1  30.0.0.1 PIM  0 ms
-2  40.0.0.1 PIM  2 ms
-3  50.0.0.1 PIM  100 ms
-4  60.0.0.1 PIM  156 ms
-5  200.0.0.1 PIM  123 ms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Manager (#)	Administrators or local user group members with execution rights for this command.

power consumption-average-period

`power consumption-average-period <PERIOD-IN-SECONDS>`

Description

Configures a time period for average power consumption in seconds.

Parameter	Description
<PERIOD-IN-SECONDS>	Specifies the period in seconds for average power consumed. Range: 60-3600. Default: 600

Example

Configuring a time period of 60 seconds for average power consumption:

```
switch(config)# power consumption-average-period 60
```

Command History

Release	Modification
10.13	Command introduced.

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	`config`	Administrators or local user group members with execution rights for this command.

show bluetooth

`show bluetooth`

Description

Shows general status information about the Bluetooth wireless management feature on the switch.

Usage

This command shows status information about the following:

- The USB Bluetooth adapter
- Clients connected using Bluetooth
- The switch Bluetooth feature.

The output of the **show running-config** command includes Bluetooth information only if the Bluetooth feature is disabled.

The device name given to the switch includes the switch serial number to uniquely identify the switch while pairing with a mobile device.

The management IP address is a private network address created for managing the switch through a Bluetooth connection.

Examples

Example output when Bluetooth is enabled but no Bluetooth adapter is connected. *<XXXX>* is the switch platform and *<NNNNNNNNNN>* is the device identifier.

```
switch# show bluetooth
Enabled              : Yes
Device name          : <XXXX>-<NNNNNNNNNN>
Adapter State        : Absent
```

Example output when Bluetooth is enabled and there is a Bluetooth adapter connected:

```
switch# show bluetooth
Enabled              : Yes
Device name          : <XXXX>-

Adapter State        : Ready
Adapter IP address   : 192.168.99.1
Adapter MAC address  : 480fcf-af153a

Connected Clients
-----------------
Name             MAC Address      IP Address     Connected Since
--------------   --------------   ------------   ------------------------
Mark's iPhone    089734-b12000    192.168.99.10  2018-07-09 08:47:22 PDT
```

Example output when Bluetooth is disabled:

```
switch# show bluetooth
Enabled              : No
Device name          : <XXXX>-<NNNNNNNNNN>
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show boot-history

```
show boot-history [all|{vsf member <1-10>}]
```

Description

Shows boot history information. When no parameters are specified, shows the most recent information about the current boot operation, and the three previous boot operations for the switch. When the **all** parameter is specified, the output of this command shows the boot information for the active management module.

.

To view boot-history on a standby, the command must be sent on the conductor console.

Parameter	Description
`all`	Optional. Shows boot information for the active management module.
`vsf member <1-10>`	Optional. Display boot history for the specified VSF member

Usage

This command displays the boot-index, boot-ID, and up time in seconds for the current boot. If there is a previous boot, it displays boot-index, boot-ID, reboot time (based on the time zone configured in the system) and reboot reasons. Previous boot information is displayed in reverse chronological order.

The output of this command includes the following information:

Parameter	Description
`Index`	The position of the boot in the history file. Range: 0 to 3.

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
```

Showing the boot history of the active management module and all line modules:

```
switch#
Management module
==================

Index : 3
Boot ID : f1bf071bdd04492bbf8439c6e479d612
Current Boot, up for 22 hrs 12 mins 22 secs

Index : 2
Boot ID : edfa2d6598d24e989668306c4a56a06d
07 Aug 18 16:28:01 : Reboot requested through database

Index : 1
Boot ID : 0bda8d0361df4a7e8e3acdc1dba5caad
07 Aug 18 14:08:46 : Reboot requested through database

Index : 0
Boot ID : 23da2b0e26d048d7b3f4b6721b69c110
07 Aug 18 13:00:46 : Reboot requested through database

Line module 1/1
==================
Index : 3
10 Aug 17 12:45:46 : dune_agent crashed
...

Management module
==================

Index : 3
Boot ID : f1bf071bdd04492bbf8439c6e479d612
Current Boot, up for 22 hrs 12 mins 22 secs

Index : 2
Boot ID : edfa2d6598d24e989668306c4a56a06d
07 Aug 18 16:28:01 : Reboot requested through database

Index : 1
Boot ID : 0bda8d0361df4a7e8e3acdc1dba5caad
07 Aug 18 14:08:46 : Reboot requested through database

Index : 0
Boot ID : 23da2b0e26d048d7b3f4b6721b69c110
07 Aug 18 13:00:46 : Reboot requested through database

Line module 1/1
==================
Index : 3
10 Aug 17 12:45:46 : dune_agent crashed
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show capacities

```
show capacities <FEATURE> [vsx-peer]
```

Description

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

Parameter	Description
<FEATURE>	Specifies a feature. For example, **aaa** or **vrrp**.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Capacities are expressed in user-understandable terms. Thus they may not map to a specific hardware or software resource or component. They are not intended to define a feature exhaustively.

Examples

Showing all available capacities for BGP:

```
switch# show capacities bgp

System Capacities: Filter BGP
Capacities Name                                                                    Value
--------------------------------------------------------------------------------------
-
Maximum number of AS numbers in as-path attribute
32
...
```

Showing all available capacities for mirroring:

```
switch# show capacities mirroring

System Capacities: Filter Mirroring
Capacities Name                                                                    Value
--------------------------------------------------------------------------------------
-
Maximum number of Mirror Sessions configurable in a system
4
Maximum number of enabled Mirror Sessions in a system
4
```

Showing all available capacities for MSTP:

```
switch# show capacities mstp

System Capacities: Filter MSTP
Capacities Name                                                                 Value
--------------------------------------------------------------------------------
-
Maximum number of mstp instances configurable in a system
64
```

Showing all available capacities for VLAN count:

```
switch# show capacities vlan-count

System Capacities: Filter VLAN Count
Capacities Name                                                                 Value
--------------------------------------------------------------------------------
-
Maximum number of VLANs supported in the system
4094
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show capacities-status

`show capacities-status <FEATURE> [vsx-peer]`

Description

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

Parameter	Description
<FEATURE>	Specifies the feature, for example **aaa** or **vrrp** for which to display capacities, values, and status. Required.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the system capacities status for all features:

```
switch# show capacities-status

System Capacities Status
Capacities Status Name                                                    Value Maximum
------------------------------------------------------------------------------------
Number of active gateway mac addresses in a system                        0      16
Number of aspath-lists configured                                         0      64
Number of community-lists configured                                      0      64
...
```

Showing the system capacities status for BGP:

```
switch# show capacities-status bgp

System Capacities Status: Filter BGP
Capacities Status Name                                                     Value Maximum
-------------------------------------------------------------------------------------
Number of aspath-lists configured                                          0      64
Number of community-lists configured                                       0      64
Number of neighbors configured across all VRFs                             0      50
Number of peer groups configured across all VRFs                           0      25
Number of prefix-lists configured                                          0      64
Number of route-maps configured                                            0      64
Number of routes in BGP RIB                                                0  256000
Number of route reflector clients configured across all VRFs               0      16
```

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
```

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
================================================================================
```

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.
```

Command History

Release	Modification
10.14	Command introduced.

Command Information

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

show domain-name

```
show domain-name [vsx-peer]
```

Description

Shows the current domain name.

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

Usage

If there is no domain name configured, the CLI displays a blank line.

Example

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show environment fan

```
show environment fan [vsx-peer]
```

Description

Shows the status information for all fans and fan trays (if present) in the system.

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

Usage

For fan trays, **Status** is one of the following values:

- ready:The fan tray is operating normally.
- fault:The fan tray is in a fault event. The status of the fan tray does not indicate the status of fans.
- empty:The fan tray is not installed in the system.

For fans:

```
Speed :Indicates the relative speed of the fan based on the nominal speed range of the
fan. Values are:
   Slow:The fan is running at less than 25% of its maximum speed.
   Normal:The fan is running at 25-49% of its maximum speed.
   Medium:The fan is running at 50-74% of its maximum speed.
   Fast:The fan is running at 75-99% of its maximum speed.
   Max:The fan is running at 100% of its maximum speed.
   N/A:The fan is not installed.
Direction: The direction of airflow through the fan. Values are:
   front-to-back:Air flows from the front of the system to the back of the system.
   N/A:The fan is not installed.
Status: Fan status. Values are:
   uninitialized:The fan has not completed initialization.
   ok: The fan is operating normally.
   fault: The fan is in a fault state.
   empty: The fan is not installed.
```

Examples

Showing output for a system without a fan tray:

```
switch# show environment fan

Fan information
-------------------------------------------------------------------
Fan    Serial Number  Speed   Direction      Status        RPM
```

```
-------------------------------------------------------------------
1     SGXXXXXXXXXX   slow    front-to-back  ok            6000
2     SGXXXXXXXXXX   normal  front-to-back  ok            8000
3     SGXXXXXXXXXX   medium  front-to-back  ok            11000
4     SGXXXXXXXXXX   fast    front-to-back  ok            14000
5     SGXXXXXXXXXX   max     front-to-back  fault         16500
6     N/A            N/A     N/A            empty
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show environment led

```
show environment led [vsx-peer]
```

Description

Shows state and status information for all the configurable LEDs in the system.

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

Example

Showing state and status for LED:

```
switch# show environment led
Name           State     Status
-----------------------------------
locator        flashing  ok
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show environment power-consumption

```
show environment power-consumption [detail]
```

Description

Displays power consumption information.

Parameter	Description
[detail}	Displays detailed power consumption information.
<MEMBER-ID>	For VSF supported platforms only. Displays the power consumption information for the specified VSF member. Range: 1-10.

Usage

Power consumed values are updated every 5 seconds. The total power consumed is the total power used in a chassis. The power consumed average is calculated from the total power consumed as a running average over a period of time. The average period has a default of 10 minutes. The period can be configured using **power-consumption-average-period.**

On chassis where power input is not supported, power consumed is displayed as Power Usage and PSU Output Power is displayed as N/A.

The following information is provided for a summary of power consumption:

- line module: power used by line module
- management module: power used by management module
- fabric module: power used by fabric module
- chassis module: power used by chassis module
- fan module: power used by fan module
- power total: total power consumption
- average power: average for total power consumption that is calculated over a given period
- average period: time to calculate power average

For more information, see the video AOS-CX 10.14 Release Update: Sustainability Update.

Example

Showing the power consumption for a 1RU switch:

```
switch# show environment power-consumption

Power Consumption Averaging Period : 600 seconds
```

```
                                      Power Usage (W)      PSU Output (W)
Name Description                     Instant   Average   Instant   Average
-------------------------------------------------------------------------------
1    8360-32Y4C v2 Switch             120.00    111.16    111.00    102.62
```

Showing the power consumption for a VSF stack:

```
switch# show environment power-consumption

Power Consumption Averaging Period : 600 seconds

                                      Power Usage (W)      PSU Output (W)
Name Description                     Instant   Average   Instant   Average
-------------------------------------------------------------------------------
1    6200M 24G 4SFP+ Sw               350.00    349.62    300.00    311.50
2    6200M 24G 4SFP+ Sw               300.00    299.50    280.00    275.50
```

Showing the power consumption for a switch where input reading is not supported:

```
switch# show environment power-consumption

Power Consumption Averaging Period : 600 seconds

                                      Power Usage (W)      PSU Output (W)
Name Description                     Instant   Average   Instant   Average
-------------------------------------------------------------------------------
1    6200M 24G 4SFP+ Sw               321.00    330.30       N/A       N/A
```

Showing the power consumption for a switch with multiple line cards, in brief:

```
switch# show environment power-consumption
Power Consumption Averaging Period : 600 seconds

                                      Power Usage (W)      PSU Output (W)
Name Description                     Instant   Average   Instant   Average
-------------------------------------------------------------------------------
1    6410 v2 Chassis                  900.00    905.62    798.00    803.23
```

Showing the power consumption for a switch with multiple line cards, in detail:

```
switch# show environment power-consumption detail
Power Consumption Averaging Period : 600 seconds

                         Power Usage (W)      PSU Output (W)
Name Module Type        Instant   Average   Instant   Average
-------------------------------------------------------------
1    chassis total     1495.00   1499.99   1307.00   1300.67
1/3   line               97.00
1/4   line               95.00
1/5   line               90.00
1/6   line               58.00
1/7   line               90.00
1/8   line               93.00
1/9   line               96.00
1/10  line               92.00
```

```
1/11  line              100.00
1/12  line               99.00
1/1   management         14.00
1/2   management         13.00
      other             370.00
```

Showing the power consumption for 4 member stack, in detail:

```
switch# show environment power-consumption detail

Power Consumption Averaging Period : 600 seconds

                         Power Usage (W)      PSU Output (W)
Name Module Type       Instant   Average   Instant   Average
-------------------------------------------------------------
1    chassis total      930.00    905.17    830.00    803.40
2    chassis total      900.00    920.00    875.00    880.25
3    chassis total      850.00    857.25    802.00    805.00
4    chassis total     1200.00   1100.56    921.00    950.00

Total Power Consumption      3428.00
```

Showing the power consumption for VSF member 2:

```
switch# show environment power-consumption member 2

Power Consumption Averaging Period : 600 seconds

                                     Power Usage (W)      PSU Output (W)
Name Description                   Instant   Average   Instant   Average
-------------------------------------------------------------------------
2    6200M 24G 4SFP+ Sw             300.00    299.50    280.00    275.50
```

Showing the power consumption for VSF invalid member:

```
switch# show environment power-consumption member 5
Member 5 is not present
```

Command History

Release	Modification
10.14.1000	Introduced enhancement to power consumption and power consumption average.
10.13	Command introduced.

Command Information

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

show environment power-redundancy

```
show environment power-consumption [vsx-peer]
```

Description

Displays power consumption information.

Parameter	Description
[vsx-peer]	Optional. Display switch power redundancy informationfor a VSX peer.

Example

Showing the power redundancy is not configured

```
switch# # show env power-redundancy
Configured  Operational
Redundancy  Redundancy
-------------------------
n+n         none
```

Command History

Release	Modification
10.16	Command introduced.

Command Information

Platforms	Command context	Authority
8325 8325P 9300 9300S	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show environment power-supply

```
show environment power-supply
  vsx-peer
  input-voltage environment
```

Description

Shows status information about all power supplies in the switch.

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

Parameter	Description
`input-voltage`	Display the statistic and status of the Power Supply Unit (PSU) input voltage. This parameter is supported on 5420, 6200, 6300M/6300F, 6400, 8320, 8325/8325H/8325P, 8100, 8360, 8400, 9300/9300S and 10000 Switch series.

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 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.

If you include the optional **input-voltage** parameter, the output includes the following information:

Output Column	Description

Output Column	Description

Example

The output of the following command shows input voltage data for a power supply. In the following example, the output of the **show environment power-supply input-voltage** command has been broken into two sections to better fit in this document. In the product command-line interface, the output appears as a single, wide table.

```
switch# show environment power-supply input-voltage
Input Voltage Averaging Period : 15 minutes

-------------------------------------------------------------------------
         Product  Input   Voltage     Instantaneous  Average Input Voltage
Mbr/PSU  Number   Type    Range       Input Voltage
-------------------------------------------------------------------------
1/1      JL087A   AC      110V-240V  123.406        123.000
1/2      JL670A   AC      110V-179V  119.750        119.000

-------------------------------------------------------------------------
Last Input Violation         Input Voltage   Last Input Recovery
Timestamp                    Recovery        Timestamp
-------------------------------------------------------------------------
Wed Nov 06 08:51:14 UTC 2024 2               Wed Nov 06 08:51:14 UTC 2024
Wed Nov 06 08:51:14 UTC 2024 2               Wed Nov 06 08:51:14 UTC 2024
```

Command History

Release	Modification
10.16.1000	The input-voltage environment parameter is introduced.
10.07 or earlier	--

Command Information

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

show environment temperature

```
show environment temperature [detail] [vsx-peer]
```

Description

Shows the temperature information from sensors in the switch that affect fan control.

Parameter	Description
`detail`	Shows detailed information from each temperature sensor.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Temperatures are shown in Celsius.

Valid values for status are the following: \

Parameter	Description
`normal`	Sensor is within nominal temperature range.
`max`	Highest temperature from this sensor.
`low_critical`	Lowest threshold temperature for this sensor.
`critical`	Highest threshold temperature for this sensor.
`fault`	Fault event for this sensor.
`emergency`	Over temperature event for Over temperature event for this sensor.

Examples

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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show hostname

```
show hostname [vsx-peer]
```

Description

Shows the current host name.

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

Example

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show images

```
show images [vsx-peer]
```

Description

Shows information about the software in the primary and secondary images.

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

Example

Showing the primary and secondary images on a 8320 switch:

```
switch# show images
--------------------------------------------------------------------------------
AOS-CX Primary Image
--------------------------------------------------------------------------------
Version : TL.10.05.0001I
Size    : 405 MB
Date    : 2020-04-23 02:49:04 PDT
SHA-256 : 7efe86a445e87e40f47de156add25720b7277cae1a8db2f9c4ea5f49e74f2a5a

--------------------------------------------------------------------------------
AOS-CX Secondary Image
--------------------------------------------------------------------------------
Version : TL.10.05.0001I
Size    : 405 MB
Date    : 2020-04-23 02:49:04 PDT
SHA-256 : 7efe86a445e87e40f47de156add25720b7277cae1a8db2f9c4ea5f49e74f2a5a

Default Image : primary

------------------------------------------------------
Management Module 1/1 (Active)
------------------------------------------------------
Active Image       : primary
Service OS Version : TL.01.05.0002-internal
BIOS Version       : TL-01-0013
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip errors

```
show ip errors [{vrf <vrf-name>}|all-vrfs]
```

Description

Shows harware and software IP error statistics for packets received by the switch since the switch was last booted. If none of the optoinal VRF parameters are included, the **show ip errors** command displays the current system-wide hardware IP error counters and the default VRF's software IP error counters on the switch

Parameter	Description
`vrf <vrf-name>`	Optional. Display hardware and software IP error counters for a specific VRF.
`all-vrfs`	Optional. Display hardware and software IP error counters for all VRFs

Usage

IP error info about received packets is collected from each active line card on the switch and is preserved during failover events. Error counts are cleared when the switch is rebooted.

Drop reasons may include the following:

- **Malformed packet**

  The packet does not conform to TCP/IP protocol standards such as packet length or internet header length.

  A large number of malformed packets can indicate that there are hardware malfunctions such as loose cables, network card malfunctions, or that a DOS (denial of service) attack is occurring.

- **IP address error**

  The packet has an error in the destination or source IP address. Examples of IP address errors include the following:

  - The source IP address and destination IP address are the same.
  - There is no destination IP address.
  - The source IP address is a multicast IP address.
  - The forwarding header of an IPv6 address is empty.
  - There is no source IP address for an IPv6 packet.

- **Invalid TTLs**

  The TTL (time to live) value of the packet reached zero. The packet was discarded because it traversed the maximum number of hops permitted by the TTL value.

  TTLs are used to prevent packets from being circulated on the network endlessly.

Example

Showing the current system-wide hardware IP error counters and the default VRF's software IP error counters on the switch:

```
switch# show ip errors
System-wide (hardware) IP errors
-------------------------------------------------
Drop reason                                Packets
-------------------------------------------------
Malformed packets                                1
IP address errors                               10
Per-VRF (software) IP errors
-------------------------------------------------
VRF
Drop reason                              Packets
-------------------------------------------------
default
IPv4 maximum transmission unit                 3
IPv4 time to live                              0
IPv6 maximum transmission unit                 0
IPv6 hop limit                                 6
------------------------------
Malformed packets               1


...
```

Shoiwng the current system-wide hardware IP error counter and the software IP error counter for all VRFs on the switch.

```
switch# show ip errors all-vrfs
System-wide (hardware) IP errors
-------------------------------------------------
Drop reason                                Packets
-------------------------------------------------
Malformed packets                                1
IP address errors                               10
Per-VRF (software) IP errors
-------------------------------------------------
VRF
Drop reason                              Packets
-------------------------------------------------
default
IPv4 maximum transmission unit                 3
IPv4 time to live                              0
IPv6 maximum transmission unit                 0
IPv6 hop limit                                 6
red
IPv4 maximum transmission unit                 3
IPv4 time to live                              7
IPv6 maximum transmission unit                 0
IPv6 hop limit                                 6
blue
```

```
IPv4 maximum transmission unit               0
IPv4 time to live                            1
IPv6 maximum transmission unit               0
IPv6 hop limit                               6

...
```

Command History

Release	Modification
10.14.1000	Command updated to display both hardware and software IP errors in the command output.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8100 8320 8325 8325H 8325P 8360 9300 9300S 10000	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show module

```
show module [vsx-peer]
```

Description

Shows information about installed line modules and management modules.

Although this switch does not have removable modules, this command will still return information about the switch, referring to management modules and line modules.

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

Usage

Identifies and shows status information about the line modules and management modules that are installed in the switch.

To show the configuration information—if any—associated with that line module slot, use the **show running-configuration** command.

Status is one of the following values:

`Active`
This switch is the active management module.

`Standby`
This switch is the standby management module.

`Deinitializing`
The switch is being deinitialized.

`Diagnostic`
The switch is in a state used for troubleshooting.

`Down`
The switch is physically present but is powered down.

`Empty`
The switch hardware is not installed in the chassis.

`Failed`
The switch has experienced an error and failed.

`Failover`
This switch is a fabric module or a line module, and it is in the process of connecting to the new active management module during a management module failover event.

`Initializing`
The switch is being initialized.

`Present`
The switch hardware is installed in the chassis.

`Ready`
The switch is available for use.

`Updating`
A firmware update is being applied to the switch.

Examples

Showing all installed modules on an 8320 switch:

```
switch(config)# show module

Management Modules
==================

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL581A  8320 Mgmt Mod                      TW87KCW00X Ready


Line Modules
============

     Product                                    Serial
Name Number  Description                        Number     Status
---- ------- ---------------------------------- ---------- ----------------
1/1  JL581A  8320                               TW87KCW00X Ready
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show running-config

`show running-config [<FEATURE>] [all] [vsx-peer]`

Description

Shows the current nondefault configuration running on the switch. No user information is displayed.

Parameter	Description
<FEATURE>	Specifies the name of a feature. For a list of feature names, enter the `show running-config` command, followed by a space, followed by a question mark (?). When the `json` parameter is used, the `vsx-peer` parameter is not applicable.
all	Shows all default values for the current running configuration.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version AOS-CX 10.0X.XXXX
!
lldp enable
linecard-module LC1 part-number JL363A
vrf green
!
!
!
!
!
!
aaa authentication login default local
aaa authorization commands default none
!
!
!
!
vlan 1
    no shutdown
vlan 20
    no shutdown
```

```
vlan 30
    no shutdown
interface 1/1/1
    no shutdown
    no routing
    vlan access 30
interface 1/1/32
    no shutdown
    no routing
    vlan access 20
interface bridge_normal-1
    no shutdown
interface bridge_normal-2
    no shutdown
interface vlan20
    no shutdown
    vrf attach green
    ip address 20.0.0.44/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable

interface vlan30
    no shutdown
    vrf attach green
    ip address 30.0.0.44/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable

    ip pim-sparse hello-interval 100
```

Showing the current running configuration in json format:

```
switch> show running-config json
Running-configuration in JSON:
{
    "Monitoring_Policy_Script": {
        "system_resource_monitor_mm1.1.0": {
            "Monitoring_Policy_Instance": {
                "system_resource_monitor_mm1.1.0/system_resource_monitor_
mm1.1.0.default": {
                    "name": "system_resource_monitor_mm1.1.0.default",
                    "origin": "system",
                    "parameters_values": {
                        "long_term_high_threshold": "70",
                        "long_term_normal_threshold": "60",
                        "long_term_time_period": "480",
                        "medium_term_high_threshold": "80",
                        "medium_term_normal_threshold": "60",
                        "medium_term_time_period": "120",
                        "short_term_high_threshold": "90",
                        "short_term_normal_threshold": "80",
                        "short_term_time_period": "5"
                    }
                }
            },
...
...
...
...
```

Show the current running configuration without default values:

```
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
!
!
!
!
vlan 1
switch(config)# show running-config all
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
!
!
!
!
vlan 1
switch(config)#
```

Show the current running configuration with default values:

```
switch(config)# snmp-server vrf mgmt
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
snmp-server vrf mgmt
!
!
!
!
!
vlan 1
switch(config)#
switch(config)#
switch(config)# show running-config all
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
```

```
!
snmp-server vrf mgmt
snmp-server agent-port 161
snmp-server community public
!
!
!
!
!
vlan 1
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show running-config current-context

`show running-config current-context`

Description

Shows the current non-default configuration running on the switch in the current command context.

Usage

You can enter this command from the following configuration contexts:

- Any child of the global configuration (**config**) context. If the child context has instances—such as interfaces—you can enter the command in the context of a specific instance. Support for this command is provided for one level below the **config** context. For example, entering this command for a child of a child of the `config` context not supported. If you enter the command on a child of the **config** context, the current configuration of that context and the children of that context are displayed.
- The global configuration (**config**) context. If you enter this command in the global configuration (**config**) context, it shows the running configuration of the entire switch. Use the **show running-configuration** command instead.

Examples

Showing the running configuration for the current interface:

```
switch(config-if)# show running-config current-context
interface 1/1/1
vsx-sync qos vlans
```

```
    no shutdown
    description Example interface
    no routing
vlan access 1
    exit
```

Showing the current running configuration for the management interface:

```
switch(config-if-mgmt)# show running-config current-context
interface mgmt
    no shutdown
    ip static 10.0.0.1/24
    default-gateway 10.0.0.8
    nameserver 10.0.0.1
```

Showing the running configuration for the external storage share named **nasfiles**:

```
switch(config-external-storage-nasfiles)# show running-config current-context
external-storage nasfiles
   address 192.168.0.1
   vrf default
   username nasuser
   password ciphertext
AQBapalKj+XMsZumHEwIc9OR6YcOw5Z6Bh9rV+9ZtKDKzvbaBAAAAB1CTrM=
   type scp
   directory /home/nas
   enable
switch(config-external-storage-nasfiles)#
```

Showing the running configuration for a context that does not have instances:

```
switch(config-vsx)# show run current-context
vsx
    inter-switch-link 1/1/1
    role secondary
    vsx-sync sflow time
```

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 non-JSON format for an 8320 switch:

```
Leaf2(config)# show startup-config
Startup configuration:
!
!Version AOS-CX TL.xx.xx.xxxx
hostname Leaf2
user admin group administrators password ciphertext

AQBapaGi+KZp4g8gw63UqK+zCtvO5zigFLv2DFBEH+lztqjdYgAAABwrJ+5GayUWArgv9tVFo9AzMY6gmI
7x/

KBEkGBJDXjpFson2qM83CXBUI673qWHDQ0pEIZXeuig0XogCVuId4oZiQVZlOe2MfxnqZL+E9hXaMNVowB
wbD0
cli-session
    timeout 0
!
!
!
ssh server vrf mgmt
```

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"
        }
    },
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show system

```
show system [serviceos password-prompt] [vsx-peer]
```

Description

Shows general status information about the system.

Parameter	Description
`serviceos password-prompt`	Shows the Service OS password prompt status.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

CPU utilization represents the average utilization across all the CPU cores.

System Description, System Contact, and System Location can be set with the `snmp-server` command.

When `vsx-peer` is specified, the `Up Time` value is not shown because it is not synchronized between VSX peers.

Examples

Showing system information:

```
switch# show system
Hostname               : switch
System Description     : switch description
System Contact         : contact
System Location        : location

Vendor                 : Aruba
Product Name           : Xxxxxx ...
Chassis Serial Nbr     : 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
```

Showing system information for a VSX primary and secondary (peer) switch:

```
switch# show system
Hostname                : vsx-primary
System Description      : switch description
System Contact          : contact
System Location         : location

Vendor                  : Aruba
Product Name            : Xxxxxx ...
Chassis Serial Nbr      : XXXXXXXXXX
Base MAC Address        : xxxxxx-xxxxxx

Hostname                : vsx-primary
System Description      : switch description
System Contact          : contact
System Location         : location

Vendor                  : Aruba
Product Name            : Xxxxxx ...
Chassis Serial Nbr      : XXXXXXXXXX
Base MAC Address        : xxxxxx-xxxxxx
AOS-CX Version          : XX.99.99.9999

Time Zone               : UTC

Up Time                 : 1 week, 2 hours, 15 minutes
CPU Util (%)            : 15
CPU Util (% avg 1 min)  : 12
CPU Util (% avg 5 min)  : 8
Memory Usage (%)        : 37


switch# show system vsx-peer
Hostname                : vsx-secondary
System Description      : switch description
System Contact          : contact
System Location         : location

Vendor                  : Aruba
Product Name            : Xxxxxx ...
Chassis Serial Nbr      : XXXXXXXXXX
Base MAC Address        : xxxxxx-xxxxxx
AOS-CX Version          : XX.99.99.9999

Time Zone               : UTC

CPU Util (%)            : 7
CPU Util (% avg 1 min)  : 13
CPU Util (% avg 5 min)  : 9
Memory Usage (%)        : 32
```

Command History

Release	Modification
10.12	Added `CPU Util (% avg 1 min)` and `CPU Util (% avg 5 min)`.
10.07 or earlier	--

Command Information

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

show system resource-utilization

`show system resource-utilization [all | daemon <DAEMON-NAME>] [vsx-peer]`

Description

Shows the system resource utilization data.

Parameter	Description
`all`	Shows the resource utilization data for the entire switch.
`daemon <DAEMON-NAME>`	Shows only the resource utilization data for the process identified by *<DAEMON-NAME>*.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

For a list of daemons that log events, enter `show events -d ?` from a switch prompt in the manager (#) context.

Examples

Showing system resource utilization data:

```
switch# show system resource-utilization
System Resources:
Processes                          :  144
CPU usage(%)                       :   10
CPU usage(% average over 1 minute) :   11
CPU usage(% average over 5 minute) :   15
Memory usage(%)                    :   22
Open FD's                          : 1358
Storage 1: Endurance utilization = 10-20% (mmc-type-a), 0-10% (mmc-type-b),
   Health = normal
```

```
Data written to various partitions since boot
Nos      :   5 MB
Log      :   1 MB
Coredump :  23 MB
Security :   2 MB
Selftest : 405 KB
Swap     :  14 MB

Storage partition usage(%)
Nos      :   5
Log      :  60
Coredump :  23
Security :   2
Selftest :   1
Swap     :   0

Process                 CPU Usage(%)    Memory Usage(%)   Open FD's
------------------------------------------------------------------------
hpe-sysmond                 1               2               11
hpe-mgmdd                   0               1               5
...
```

Attempting to show resource utilization data when system resource utilization polling is disabled:

```
switch# show system resource-utilization
System resource utilization data poll is currently disabled
```

Showing the resource utilization data for a particular process:

```
switch# show system resource-utilization daemon hpe-sysmond
Process                 CPU Usage(%)    Memory Usage(%)   Open FD's
------------------------------------------------------------------------
hpe-sysmond                 1               2               11
```

Showing system resource utilization data for all:

```
switch# show system resource-utilization all
------------------------------------------------------------------------
Resource utilization data for Management Module
------------------------------------------------------------------------

System Resources:
Processes                          :  244
CPU usage(%)                       :   10
CPU usage(% average over 1 minute) :   11
CPU usage(% average over 5 minute) :   15
Memory usage(%)                    :   11
Open FD's                          : 1854
Storage 1: Endurance utilization = 0-10% (mmc-type-a), 0-10% (mmc-type-b),
   Health = normal

Data written to various partitions since boot
Nos      :  15 MB
Log      :   1 MB
```

```
Coredump :  23 MB
Security :   2 MB
Selftest : 405 KB
Swap     :   0 KB

Storage partition usage(%)
Nos      :   5
Log      :  60
Coredump :  23
Security :   2
Selftest :   1
Swap     :   0

Process                  CPU Usage(%)    Memory Usage(%)   Open FD's
-------------------------------------------------------------------------
(sd-pam)                 0               0                 7
aaautilspamcfg           0               1                 10
...
```

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.
<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.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show usb

```
show usb [vsx-peer]
```

Description

Shows the USB port configuration and mount settings.

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

Examples

If USB has not been enabled:

```
switch> show usb
Enabled: No
Mounted: No
```

If USB has been enabled, but no device has been mounted:

```
switch> show usb
Enabled: Yes
Mounted: No
```

If USB has been enabled and a device mounted:

```
switch> show usb
Enabled: Yes
Mounted: Yes
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager	Operators or Administrators or local user group members with

Platforms	Command context	Authority
	(#)	execution rights for this command. Operators can execute this command from the operator context (>) only.

show 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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show version

```
show version [vsx-peer]
```

Description

Shows version information about the network operating system software, service operating system software, and BIOS.

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

Example

Showing version information for an 8360 switch:

```
(8360)> show version
--------------------------------------------------------------------------------
ArubaOS-CX
(c) Copyright 2017-2023 Hewlett Packard Enterprise Development LP
--------------------------------------------------------------------------------
Version      : LL.10.13.0005C
Build Date   : 2023-10-20 23:26:43 UTC
Build ID     : ArubaOS-CX:LL.10.13.0005C:d09961efb102:202310202257
```

```
Build SHA    : d09961efb1026366961fa11d71817e67bb38b9f4
Hot Patches  :
Active Image : secondary
Service OS Version : LL.01.12.0004
BIOS Version       : LL.01.0001
```

Showing version information for an 8320 switch:

```
switch(config)# show version
--------------------------------------------------------------------------------
AOS-CX
(c) Copyright 2017-2022 Hewlett Packard Enterprise Development LP
--------------------------------------------------------------------------------
Version      : TL.xx.xx.xxxx
Build Date   : 2022-05-27 17:00:46 PDT
Build ID     : AOS-CX:xx.xx.xxxx:feb590a400a5:201908201736
Build SHA    : feb590a400a57ed818b01614f92010d74fbc9a4b
Active Image : secondary

Service OS Version : TL.01.03.0008
BIOS Version       : TL-01-0013
```

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
```

Command History

Release	Modification
10.07 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
...
```

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
...
```

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
```

Command History

Release	Modification
10.07 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
```

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 19

Support and Other Resources

Accessing HPE Aruba Networking Support

HPE Aruba Networking Support Services	https://www.hpe.com/us/en/networking/hpe-aruba-networking-support-services.html
AOS-CX Switch Software Documentation Portal	https://arubanetworking.hpe.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) +1-650-750-0350 (Backup—Toll Number)
International telephone	https://www.hpe.com/psnow/doc/a50011948enw

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

HPE Aruba Networking Developer Hub	https://developer.arubanetworks.com/hpe-aruba-networking-aoscx/docs/about
Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Software Technical Update channel on YouTube.	Videos on new features introduced in this release: https://www.youtube.com/playlist?list=PLsYGHuNuBZcbWPEjjHuVMqP-Q_UL3CskS

HPE Aruba Networking Hardware Documentation and Translations Portal	https://arubanetworking.hpe.com/techdocs/hardware/DocumentationPortal/Content/home.htm
HPE Aruba Networking software	https://networkingsupport.hpe.com/downloads
Software licensing and Feature Packs	https://licensemanagement.hpe.com/
End-of-Life information	https://networkingsupport.hpe.com/end-of-life

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.