

AOS-CX 10.17 Fundamentals Guide

8400 Switch Series



**Hewlett Packard
Enterprise**

Published: November 2025

Version: 1

Copyright Information

© Copyright 2025 Hewlett Packard Enterprise Development LP.

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

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



Notices

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

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

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

Acknowledgments

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

About this document	11
Applicable products	11
Latest version available online	11
Command syntax notation conventions	11
About the examples	12
Identifying switch ports and interfaces	12
Identifying modular switch components	13
About AOS-CX	14
AOS-CX system databases	14
Network Analytics Engine introduction	15
AOS-CX CLI	15
HPE Aruba Networking Installer mobile app	15
HPE Aruba Networking NetEdit	15
Ansible modules	16
AOS-CX Web UI	16
AOS-CX REST API	16
In-band and out-of-band management	16
SNMP-based management support	17
User accounts	17
Initial Configuration	18
Initial configuration using ZTP	18
Initial configuration using the HPE Aruba Networking Installer mobile app	19
Troubleshooting Bluetooth connections	20
Bluetooth connection IP addresses	20
Bluetooth is connected but the switch is not reachable	21
Bluetooth is not connected	21
Initial configuration using the CLI	24
Connecting to the console port	24
Connecting to the management port	25
Logging into the switch for the first time	26
Setting switch time using the NTP client	26
Configuring banners	27
Configuring in-band management on a data port	28
Using the Web UI	28
Configuring the management interface	28
Restoring the switch to factory default settings	29
Limitations and considerations	31
REST API profile switching procedure	32
Management interface commands	32
default-gateway	32
ip static	33
nameserver	34
show interface mgmt	35
NTP commands	35
ntp authentication	35
ntp authentication-key	36
ntp disable	38

ntp enable	38
ntp conductor	39
ntp server	40
ntp trusted-key	42
ntp vrf	42
show ntp associations	43
show ntp authentication-keys	44
show ntp servers	45
show ntp statistics	46
show ntp status	47
client-probe autogen-probe-file force-regen	48
autogen-enable	48
autogen-probe-file	49
show client probe autogen-probe-file	50
vans	52
name	53
Telnet access	55
Telnet commands	55
show telnet server	55
show telnet server sessions	56
telnet server	57
Interface configuration	58
Configuring a layer 2 interface	58
Configuring a layer 3 interface	58
Single source IP address	59
Priority-based flow control (PFC)	59
Flow control and lossless buffering	60
Requirements for proper lossless buffering	60
Forward error correction	60
Unsupported transceiver support	61
Configuring an interface persona	61
Modes	62
Predefined and custom persona names	63
Creating and configuring an interface persona	63
Examples	63
Modes	64
Predefined and custom persona names	65
Creating and configuring an interface persona	65
Examples	65
Monitor mode	66
Interface commands	66
allow-unsupported-transceiver	66
default interface	68
description	69
error-control	69
flow-control	70
interface	72
interface loopback	73
interface vlan	74
ip address	74
ip mtu	75
ip source-interface	76
ip tcp mss	78
ip unnumbered	79

ipv6 address	81
ipv6 source-interface	82
ipv6 tcp mss	83
l3-counters	84
mtu	85
persona	86
rate-interval	88
routing	90
show allow-unsupported-transceiver	90
show interface	91
show interface dom	98
show interface flow-control	99
show interface link-diagnostics	104
show interface statistics	106
show interface transceiver	109
show interface supported-transceivers	113
show interface utilization	116
show ip interface	117
show ip source-interface	118
show ipv6 interface	119
show ipv6 source-interface	121
shutdown	122
split	123
system interface-group	125
Source interface selection	126
Source-interface selection commands	126
ip source-interface	126
ipv6 source-interface dns	128
ipv6 source-interface	129
show ip source-interface	131
show ipv6 source-interface	133
show running-config	134
VLANs	136
Configuration and firmware management	137
Upgrade and downgrade scenarios	137
Upgrades	137
Downgrades	137
Limitations	137
REST Use Case Examples	138
Hot-patch software	144
Checkpoints	146
Checkpoint types	146
Maximum number of checkpoints	146
User generated checkpoints	146
System generated checkpoints	147
Supported remote file formats	147
Rollback	147
Checkpoint auto mode	147
Testing a switch configuration in checkpoint auto mode	148
Checkpoint commands	148
checkpoint auto	148
checkpoint auto confirm	149
checkpoint diff	150

checkpoint post-configuration	153
checkpoint post-configuration timeout	154
checkpoint rename	154
checkpoint rollback	155
copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL>	156
copy checkpoint <CHECKPOINT-NAME> {running-config startup-config}	157
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>	158
copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME>	158
copy <REMOTE-URL> startup-config running-config	159
copy running-config {startup-config checkpoint <CHECKPOINT-NAME>}	161
copy {running-config startup-config} <REMOTE-URL>	162
copy {running-config startup-config} <STORAGE-URL>	164
copy startup-config running-config	165
copy <STORAGE-URL> running-config	165
erase	167
show checkpoint <CHECKPOINT-NAME>	168
show checkpoint <CHECKPOINT-NAME> hash	170
show checkpoint post-configuration	171
show checkpoint	171
show checkpoint date	172
show running-config hash	173
show startup-config hash	174
write memory	174
Boot commands	175
boot fabric-module	175
boot line-module	176
boot management-module	177
boot management-module (recovery console)	178
boot set-default	180
boot system	180
show boot-history	182
Firmware management commands	185
copy {primary secondary} <REMOTE-URL>	185
copy {primary secondary} <FIRMWARE-FILENAME>	186
copy primary secondary	187
copy <REMOTE-URL>	187
copy secondary primary	189
copy <STORAGE-URL>	190
copy hot-patch	191
hot-patch	192
show hot-patch	193
gNMI commands	194
crypto pki application gnmi certificate	194
gnmi vrf	195
show gnmi	196

SNMP	197
Configuring SNMP	197
One Touch Provisioning	198
location-override-alternative	199
Troubleshooting	201
Prerequisites	201
Troubleshooting Scenarios	201
Scenario: Central location discovery	201
Scenario: Central connectivity	205
Scenario: Activate connectivity	212

Scenario: Central remote console shell	213
Scenario: Central disconnection timeout	220
Related features	222
Port filtering	224
Port filtering commands	224
DNS	225
DNS client	225
Configuring the DNS client	225
DNS client commands	227
ip dns domain-list	227
ip dns domain-name	228
ip dns host	228
ip dns server address	229
show ip dns	230
Device discovery and configuration	233
LLDP	233
LLDP agent	233
LLDP MED support	235
LLDP EEE	236
Configuring the LLDP agent	236
LLDP commands	237
clear lldp neighbors	237
clear lldp statistics	237
lldp	238
lldp dot3	239
lldp dot3 mfs	239
lldp holdtime-multiplier	240
lldp management-address vlan	241
lldp management-ip-address	242
lldp management-ipv6-address	243
lldp med	244
lldp med location	245
lldp receive	247
lldp reinit	248
lldp select-tlv	248
lldp timer	250
lldp tlv-enable	251
lldp transmit	252
lldp txdelay	253
lldp trap enable	253
show lldp configuration	256
show lldp configuration mgmt	257
show lldp local-device	258
show lldp neighbor-info	260
show lldp neighbor-info detail	263
show lldp neighbor-info mgmt	265
show lldp statistics	267
show lldp statistics mgmt	268
show lldp tlv	269
Cisco Discovery Protocol (CDP)	270
CDP support	270
CDP commands	270
cdp	271

clear cdp counters	271
clear cdp neighbor-info	272
show cdp	272
show cdp neighbor-info	273
show cdp traffic	274
show cdp voice-vlan mode	275
Zero Touch Provisioning	276
ZTP support	276
Setting up ZTP on a trusted network	278
ZTP using USB	279
ZTP process during switch boot	280
ZTP VSF switchover support	281
ZTP commands	281
show ztp information	281
ztp force provision	285
Thermal Management	286
Thermal management support	286
Transceiver Thermal Management	287
Switch system and hardware commands	290
allow-non-failsafe-updates	290
bluetooth disable	290
bluetooth enable	291
clear events	292
clear ip errors	293
console baud-rate	293
domain-name	294
fabric admin-state	295
hostname	296
led locator	297
module admin-state	298
module product-number	299
mtrace	301
power consumption-average-period	302
show bluetooth	303
show boot-history	304
show capacities	307
show capacities-status	309
show console	310
show core-dump	310
show deprecated commands	312
show domain-name	313
show environment fan	314
show environment led	316
show environment power-consumption	317
show environment power-consumption	320
show environment power-supply	322
show environment rear-display-module	324
show environment temperature	325
show events	326
show fabric	329
show hostname	331
show images	331
show ip errors	333

show module	335
show running-config	337
show running-config current-context	341
show startup-config	342
show system error-counter-monitor	344
show system	345
show system resource-utilization	347
show tech	352
show usb	353
show usb file-system	354
show version	355
system error-counter-monitor	356
system error-counter-monitor poll-interval	357
system resource-utilization poll-interval	358
top cpu	358
top memory	359
usb	359
usb mount unmount	360

Support and Other Resources	362
Accessing HPE Aruba Networking Support	362
Accessing Updates	363
Warranty Information	363
Regulatory Information	363
Documentation Feedback	363

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 8400 Switch Series (JL366A, JL363A, JL687A)

Latest version available online

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

Command syntax notation conventions

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

Convention	Usage
[]	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 8400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
 - Management modules are on the front of the switch in slots 1/5 and 1/6.
 - Line modules are on the front of the switch in slots 1/1 through 1/4, and 1/7 through 1/10.
- *port*: Physical number of a port on a line module

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

Identifying modular switch components

- Power supplies are on the front of the switch behind the bezel above the management modules. Power supplies are labeled in software in the format: *member/power supply*:
 - *member*: 1.
 - *power supply*: 1 to 4.
- Fans are on the rear of the switch and are labeled in software as: *member/tray/fan*:
 - *member*: 1.
 - *tray*: 1 to 4.
 - *fan*: 1 to 4.
- Fabric modules are not labeled on the switch but are labeled in software in the format: *member/module*:
 - *member*: 1.
 - *member*: 1 or 2.
- The display module on the rear of the switch is not labeled with a member or slot number.

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 through 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 within the system are not recommended to be used for other services. When two services use the same port there is a chance of unexpected behaviors from these services. Best practice is to use a unique port for each service across the 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

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, 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
```

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.

- 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:         xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
...

##### 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):

Bootting 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
           %             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
8400	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
8400	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
8400	config-if-mgmt	Administrators or local user group members with execution rights for this command.

show interface mgmt

show interface mgmt [vsx-peer]

Description

Shows status and configuration information for the management interface.

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

Example

```
switch# show interface mgmt

Address Mode           : static
Admin State            : up
Mac Address            : 02:42:ac:11:00:02
IPv4 address/subnet-mask : 192.168.1.10/16
Default gateway IPv4    : 192.168.1.1
IPv6 address/prefix     : 2001:db8:0:1::129/64
IPv6 link local address/prefix: fe80::7272:cfff:fe485/64
Default gateway IPv6    : 2001:db8:0:1::1
Primary Nameserver      : 2001::1
Secondary Nameserver    : 2001::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

NTP 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}
  [{ <PLAINTEXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
no ntp authentication-key <KEY-ID> {md5 | sha1}
  [{ <PLAINTEXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
```

Description

Defines an authentication key that is used to secure the exchange with an NTP time server. This command provides protection against accidentally synchronizing to a time source that is not trusted. The **no** form of this command removes the authentication key.



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

Parameter	Description
<KEY-ID>	Specifies the authentication key ID. Range: 1 to 65534.
md5	Selects MD5 key encryption.

Parameter	Description
sha1	Specifies SHA1 key encryption.
<PLAINTEXT-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
<code>vrf <VRF-NAME></code>	Specifies the VRF on which to act as conductor time source.
<code>stratum <NUMBER></code>	Specifies the stratum level at which the switch operates. Range: 1 - 15. Default: 8.

Examples

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

```
switch(config)# ntp conductor vrf primary-vry stratum 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.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config	Administrators or local user group members with execution rights for this command.

ntp server

```
ntp server <IP-ADDR> [key <KEY-NUM>] [minpoll <MIN-NUM>] [maxpoll <MAX-NUM>] [burst |
iburst] [prefer] [version <VER-NUM>]
no ntp server <IP-ADDR> <IP-ADDR> [key <KEY-NUM>] [minpoll <MIN-NUM>] [maxpoll <MAX-NUM>]
[burst | iburst] [prefer] [version <VER-NUM>]
```

Description

Defines an NTP server to use for time synchronization, or updates the settings of an existing server with new values. Up to eight servers can be defined.

The **no** form of this command removes a configured NTP server.



The default NTP version is 4; it is backwards compatible with version 3.

Parameter	Description
server <IP-ADDR>	Specifies the address of an NTP server as a DNS name, an IPv4 address (x.x.x.x), where x is a decimal number from 0 to 255, or an IPv6 address (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F. When specifying an IPv4 address, you can remove leading zeros. For example, the address 192.169.005.100 becomes 192.168.5.100 . When specifying an IPv6 address, you can use two colons (::) to represent consecutive zeros (but only once), remove leading zeros, and collapse a hextet of four zeros to a single 0. For example, this address 2222:0000:3333:0000:0000:0000:4444:0055 becomes 2222:0:3333::4444:55 .
key <KEY-NUM>	Specifies the key to use when communicating with the server. A trusted key must be defined with the command ntp authentication-key and authentication must be enabled with the command ntp authentication . Range: 1 to 65534.
minpoll <MIN-NUM>	Specifies the minimum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 6 (64 seconds).
maxpoll <MAX-NUM>	Specifies the maximum polling interval in seconds, as a power of 2. Range: 4 to 17. Default: 10 (1024 seconds).
burst	Send a burst of packets instead of just one when connected to the server. Useful for reducing phase noise when the polling interval is long.
iburst	Send a burst of six packets when not connected to the server. Useful for reducing synchronization time at startup.
prefer	Make this the preferred server.
version <VER-NUM>	Specifies the version number to use for all outgoing NTP packets. Range: 3 or 4. Default: 4.

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

Example

```
switch# show ntp associations
```

```
-----
ID          NAME          REMOTE          REF-ID ST LAST POLL REACH
-----
1           192.0.1.1          192.0.1.1      .INIT. 16   -   64    0
* 2  time.apple.com    17.253.2.253   .GPSs.  2   70  128   377
-----
```

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.

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
8400	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
8400	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
8400	config-cp	Administrators or local user group members with execution 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
8400	config	Administrators or local user group members with execution rights for this command.

vls

```

vls <VLAN-RANGE>
no vls <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)# vlangs 1,2,35,10,8  
switch(config-cp-autogen)# vlangs 50-60,80-90  
switch(config-cp-autogen)# vlangs 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
8400	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
<i>FILENAME</i>	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
8400	config-cp-autogen	Administrators or local user group members with execution rights for this command.

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
<code>vrf <VRF-NAME></code>	Specifies the Telnet sessions for a specific VRF.
<code>all-vrfs</code>	Specifies the Telnet sessions for all VRFs

Examples

Showing the Telnet session on the **default** VRF:

```
switch(config)# show telnet server sessions
TELNET sessions on VRF default:

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

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

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

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

TELNET sessions on VRF default:

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

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.

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`.

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)# 13-counters tx
switch(config-if)# 13-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.

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`.

PFC is not supported on the 8400X 32x10G module (JL363A).

PFC is not supported on the 8400X 8x40G module (JL365A) split interfaces (for example, 10G).

While interfaces with PFC configured are enabled, any change to QoS cos-map or queue-profile affecting the priority or queue used by PFC could cause the intended traffic to no longer be treated as lossless.

Before making CoS map or Queue Profile changes (see *Quality of Service Guide*), shut down all PFC interfaces, make all cos-map or queue-profile changes, reboot any line-modules with PFC interfaces, and then re-enable the PFC interfaces.

Flow control and lossless buffering

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 a queue in the queue profile.

Requirements for proper lossless buffering

The switch uses a virtual output queue (VOQ) architecture where most packet buffering for all destination ports occurs on the ingress line module. Each line module has between 1.5 and 4 GB of buffer memory with 256 MB used for traffic destined for multiple ports (Multidest) and the remainder for traffic destined for one port (Unidest). By default, all unicast packets arriving on ports of the same line module share the Unidest pool. Any packet can be dropped if the destination port VOQ has exceeded its limit. The VOQ limit is either 1 MB for JL365 modules, or 1.7 MB for JL366 and JL687 modules. The TX Drops columns of *show interface <IF-NAME>* command will display the number of drops that have occurred.

Priority-based Flow Control (PFC) reconfigures buffering. After the first interface is configured for PFC the switch will move some Unidest buffers to a new Headroom pool. Unicast traffic arriving at PFC-configured ports with the specified PCP will still use the Unidest pool with other traffic but will be marked as lossless. Lossless-marked packets will never be dropped when a destination port VOQ has exceeded its limit. All other unicast traffic arriving on non-PFC ports, or on PFC-configured ports with different PCPs also shares the Unidest pool. However, such traffic is still subject to dropping when a destination port VOQ has exceeded its limit.

Each PFC-configured-port priority is given a limit on the amount of lossless buffering it can store in the Unidest pool. The limit is either 1 MB for JL365A modules, or 1.7 Mbytes for JL366A and JL687A modules. Once the limit is exceeded, the switch will send a PFC pause frame from the port to stop further packets from arriving. Due to link propagation time and processing time on the receiving switch, additional packets in flight are allowed to be received and will be stored in the Headroom pool. The Headroom pool size is sufficient to store all packets in flight arriving after the priority pause frame is sent. The switch will periodically transmit priority pause frames until all the port's lossless packets are gone from the Headroom pool and its lossless packets in the Unidest pool go below half of the pool's capacity.

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 8400 Series Switches will enable unsupported transceivers for speeds up to 100G when running AOS-CX 10.10 or later.

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

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

Usage

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

Examples

Allowing unsupported transceivers with follow-up confirmation:

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

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

Allowing unsupported transceivers with confirmation in command syntax:

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

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

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

Disabling unsupported transceiver logging:

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

Disallowing unsupported transceivers with follow-up confirmation:

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

Continue (y/n)? y
```

Disallowing unsupported transceivers with confirmation in command syntax:

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

switch(config)#
```

Command History

Release	Modification
10.10	Up to 100G support enabled for unsupported transceivers on 8400 (up to 100G) series switches in UT mode.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config	Administrators or local user group members with execution rights for this command.

default interface

default interface <INTERFACE-ID>

Description

Sets an interface (or a range of interfaces) to factory default values.

Parameter	Description
<INTERFACE-ID>	Specifies the ID of a single interface or range of interfaces. Format: member/slot/port or member/slot/port-member/slot/port to specify a range.

Examples

Resetting an interface:

```
switch(config)# default default interface 1/1/1
```

Resetting an range of interfaces:

```
switch(config)# default default interface 1/1/1-1/1/10
```

Command History

Release	Modification
10.07 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.

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
10.11	Command enabled on 6400 and 8400 Switch Series.
10.08.1021	Command introduced.

Command Information

Platforms	Command context	Authority
8400	config-if	Administrators or local user group members with execution rights for this command.

flow-control

```
flow-control rx
no flow-control rx
flow-control priority rxtx <PRIORITY>
no flow-control priority rxtx <PRIORITY>
```

Description

Command **flow-control** enables negotiation of receive flow control on the current interface. The switch advertises RX support to the link partner. The final configuration is determined based on the capabilities of both partners.

Command **flow-control priority** enables priority-based flow control (PFC). A single priority is supported..

Each invocation of this command replaces the previous configuration.

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

Parameter	Description
<code>rx</code>	Enables the ability to cease and resume transmission when receiving IEEE 802.3x LLFC pause frames on this interface.
<code><PRIORITY></code>	Specifies the packet priority for which PFC will operate. Range: 0 to 7. One priority can be specified.

Usage (flow control)

- For interfaces that auto-negotiate, link-level flow control is subject to negotiation, plus speed and other parameters. Both ends of the link must negotiate the same flow control mode for it to be applied.
- For interfaces that do not auto-negotiate, the configured link-level flow control mode is always applied and the user is responsible for ensuring that both ends of the link are configured for the same mode.
- All members of a LAG must have the same flow control configuration.
- Lossless flow control is only supported for single destination unicast traffic. Replicated traffic (for example, broadcast, multicast, mirroring) cannot be guaranteed to be lossless.
- Lossless behavior is not supported when operating in a VSF stack configuration.

Usage (priority-based flow control (PFC))

- PFC will only operate correctly between interfaces with the same priority configuration. Traffic flow will not be lossless between interfaces with different priorities or between interfaces where one has PFC enabled and the other does not.
- 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.
- PFC is enabled for the given Priority Code Point. Only one priority may be enabled for PFC per interface. PFC is only supported on JL365A 8400X 8-port 40GbE QSFP+ Advanced Module, JL366A HPE Aruba Networking 8400X 6-port 40GbE/100GbE QSFP28 Adv Mod, and JL687A 8400X-32Y 32p 1/10/25G SFP/SFP+/SFP28 Module line modules.
- 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.

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
```

Enabling support for priority RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# flow-control priority rxtx 2
```

Disabling support for priority RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)#
```

Command History

Release	Modification
10.10	Adjusted the priority syntax.
10.07 or earlier	--

Command Information

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

interface

interface <PORT-NUM>

Description

Switches to the **config-if** context for a physical port. This is where you define the configuration settings for the logical interface associated with the physical port.

Parameter	Description
<PORT-NUM>	Specifies a physical port number. Format: member/slot/port .

Examples

Configuring an interface:

```
switch(config)# interface 1/1/1
switch(config-if)#
```

Command History

Release	Modification
10.07 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
8400	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 .

Parameter	Description
<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.

Parameter	Description
<VALUE>	Specifies the IP MTU in bytes. Range: 68 to 9198. Default: 1500.

Examples

Setting the IP MTU to 576 bytes:

```
switch(config-if)# ip mtu 576
```

Setting the IP MTU to the default value:

```
switch(config-if)# no ip mtu
```

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	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
<code>sflow tftp radius tacacs ntp syslog ubt dhcp-relay simplivity dns all</code>	Sets a single source IP address for a specific service. The <code>all</code> option sets a global address that applies to all protocols that do not have an address set. For DHCP relay, the address is used as both the source IP and GIADDR.
<code>interface <IFNAME></code>	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.
<code><IPv4-ADDR></code>	Specifies the source IP address to use for the specified service. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the <code>default</code> VRF, if the <code>vrf</code> option is not used). Specify the address in IPv4 format (<code>x.x.x.x</code>), where <code>x</code> is a decimal number from 0 to 255.
<code>vrf <VRF-NAME></code>	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-gre-if	Administrators or local user group members with execution rights for this command.

ip unnumbered

```
ip unnumbered <ifname>
no ip unnumbered <ifname>
```

Description

The IP unnumbered feature allows the switch to process IP packets without configuring a unique IP address on an interface by telling the router to use the IP address of another selected interface as the address for that link. Once set, this port will borrow the user-configured primary IPv4 address from a lender interface and use that IP address in its L3 control plane exchange.

The **no** version of this command removes IP unnumbered support for this port. Once unset, this port will remove borrowed IPv4 address.

Parameter	Description
<Ifname >	Name of the interface

Usage

The port where IP unnumbered is configured is known as the *borrower* interface. Only route-only ports can borrow an address.

The port the address is borrowed from is known as the *lender* interface. Only a loopback interface can be used as a lender interface. The unnumbered interface and lender interface must belong to the same VRF. Additionally, the lender interface for an IP unnumbered interface cannot itself be configured as unnumbered.

The following caveats apply to this feature:

- Only the primary IPv4 address can be borrowed on an IP unnumbered interface. You cannot configure a secondary IP address for an interface that is already configured as an IP unnumbered interface.
- If an IP address is configured on an interface that is already configured as an IP unnumbered interface, it will function as a normal IP interface.
- An IPv6 unnumbered configuration on the interface is not supported. If **ip unnumbered** is enabled on the interface, only the IPv4 address is borrowed. However, Any IPv6 configurations can co-exist with an ip unnumbered interface.
- An IP unnumbered interface cannot have multiple lender interfaces for the same address family.
- The **ip unnumbered** command requires that the interface borrowing the address is a routed port. The **IP unnumbered** feature is only supported on devices connected with point-to-point interfaces.

- An unnumbered IP address can not be used as tunnel source.
- The unnumbered interface and lender interface must belong to the same VRF.
- Deleting a lender interface removes all the associated IP unnumbered references.

Examples

Configuring IP unnumbered for a route-only port:

```
switch(config)# interface 1/1/1
switch(config-if)# ip unnumbered loopback1
```

The following examples 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
8400	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

Parameter	Description
	the specified VRF (which is the default VRF, if the <code>vrf</code> option is not used). Specify the IP address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.
<code>vrf <VRF-NAME></code>	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	<code>config</code>	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-gre-if	Administrators or local user group members with execution rights for this command.

l3-counters

```
l3-counters [rx | tx]
no l3-counters [rx | tx]
```

Description

Enables counters on a layer 3 interface. By default, all interfaces are layer 3. To change a layer 2 interface to layer 3, use the **routing** command.

The **no** form of this command, with no specification, disables both transmit and receive counters on a layer 3 interface. To disable transmit (**tx**) or receive (**rx**) counters only, specify the counter type you want to disable.

Parameter	Description
rx	Specifies receive counters.
tx	Specifies transmit counters.

Examples

Enabling layer 3 transmit counters on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# 13-counters tx
```

Disabling layer 3 transmit and receive counters on interface **1/1/2**:

```
switch(config)# interface 1/1/2
switch(config-if)# no 13-counters
```

Command History

Release	Modification
10.08	Added support for 13 counters on subinterfaces
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config-if	Administrators or local user group members with execution rights for this command.

mtu

```
mtu <VALUE>
no mtu
```

Description

Sets the MTU (maximum transmission unit) for an interface. This defines the maximum size of a layer 2 (Ethernet) frame. Frames larger than the MTU (1500 bytes by default) are dropped.

To support jumbo frames (frames larger than 1522 bytes), increase the MTU as required by your network. A frame size of up to 9198 bytes is supported.

The largest possible layer 1 frame will be 18 bytes larger than the MTU value to allow for link layer headers and trailers.

The **no** form of this command sets the MTU to the default value 1500.

Parameter	Description
<VALUE>	Specifies the MTU in bytes. Range: 46 to 9198. Default: 1500.

Examples

Setting the MTU on interface **1/1/1** to 1000 bytes:

```
switch(config)# interface 1/1/1
switch(config-if)# no routing
switch(config-if)# mtu 1000
```

Setting the MTU on interface **1/1/1** to the default value:

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

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.

Parameter	Description
<code>copy</code>	Specifies the mode: copies settings from the persona interface of the same name.
<code>attach</code>	Specifies the mode: attaches the specified interface to the persona interface of the same name.

Usage

- If the mode is specified, either `copy` or `attach`, the interface configuration is dependent on the interface template whose name is "access", "uplink", or "<PERSONA-NAME>". On the other hand, if the mode is not specified, then the persona is just a label in the interface, and its configuration is not modified even if the interface persona exists. When configuring the mode, one of the following options is possible:
 - The **copy** option performs a one-time copy of the template interface. Subsequent changes to the template are not copied and the 'persona' setting is just a label. If the mode is set to **copy** and the interface persona does not exist, then the CLI command fails with the message "Interface persona not found".
 - The **attach** option performs a copy of the template interface, and subsequent changes to the template interface configuration are immediately applied to all attached interfaces. The template interface does not need to exist before attaching other interfaces to it. After attaching a template, the copied settings can be modified for an individual interface. However, any change in the attached template will overwrite the modified values with the new template values.
- When a mode is specified, it should match an interface created with the command `interface persona <PERSONA-NAME>`. The only exception to this rule is when the mode is set to `attach` and the persona does not already exist.
- The mode is only available to be configured for an interface that meets the following conditions:
 - IS a physical interface
 - IS NOT a LAG member
 - IS NOT a persona interface

Examples

Configuring an access persona:

```
switch(config)# interface 1/1/1
switch(config-if)# persona access
```

Configuring an uplink persona:

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

Configuring a custom persona named "mypersona":

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

Removing the persona setting.

```
switch(config-if)# no persona
```

Copying a predefined persona name configuration to an interface:

1. Configuring the interface persona:

```
switch(config)# interface persona uplink
switch(config-if)# no shutdown
switch(config-if)# no routing
switch(config-if)# vlan access 100
switch(config-if)# exit
```

2. Applying the configuration from the persona named "mypersona" with **copy** mode:

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

Attaching a custom persona name named "mypersona" to several interfaces simultaneously:

1. Configuring an interface persona named "mypersona":

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

2. Applying the "mypersona" configuration with **attach** mode:

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

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. NOTE: The supported range for HPE Aruba Networking 6400 and 8400 Switch series is 30 - 300 seconds.

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.

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
8400	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]
```

Description

Shows active configurations and operational status information for interfaces.

Parameter	Description
<IFNAME>	Specifies a interface name.

Parameter	Description
<IFRANGE>	Specifies the port identifier range.
brief	Shows brief info in tabular format.
physical	Shows the physical connection info in tabular format.
extended	Shows additional statistics, including the tx filtered and rx filtered counters. ▪ Rx filter packets are protocol packets received when the protocol is disabled on the switch and there is only one port in the VLAN. Protocols include OSPF, PIM, RIP, LACP, and LLDP. ▪ An example of a Tx filtered packet would be a multicast packet being filtered from going out of the ingress port.
human-readable	Shows statistics rounded to the nearest power of 1000, for example, 1K, 345M, 2G. This is available only in the CLI interface output.
non-zero	Shows only non zero statistics.
LAG	Shows LAG interface information.
monitor	Continuously monitor interface statistics.
LOOPBACK	Shows loopback interface information.
TUNNEL	Shows tunnel interface information.
VLAN	Shows VLAN interface information.
<LAG-ID>	Specifies the LAG number. Range: 1-256
<LOOPBACK-ID>	Specifies the LOOPBACK number. Range: 0-255
<TUNNEL-ID>	Specifies the tunnel ID. Range: 1-255
<VLAN-ID>	Specifies the VLAN ID. Range: 1-4094
VXLAN	Shows the VXLAN interface information.
<VXLAN-ID>	Specifies the VXLAN interface identifier. Default: 1

Examples

Showing interface information when it is configured as a route-only port:

```
switch# show interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Link state: up for 2 days (since Sun Jun 21 05:30:22 UTC 2020)
Link transitions: 1
Description: backup data center link
Hardware: Ethernet, MAC Address: 70:72:cf:fd:e7:b4
MTU 1500
Type 1GbT
```

```

Full-duplex
qos trust none
Speed 1000 Mb/s
Auto-negotiation is on
Flow-control: off
Error-control: off
L3 Counters: Rx Enabled, Tx Enabled
Rate collection interval: 300 seconds

```

Rates	RX	TX	Total (RX+TX)
Mbits / sec	0.00	0.00	0.00
KPkts / sec	0.00	0.00	0.00
Unicast	0.00	0.00	0.00
Multicast	0.00	0.00	0.00
Broadcast	0.00	0.00	0.00
Utilization %	0.00	0.00	0.00

Statistics	RX	TX	Total
Packets	0	0	0
Unicast	0	0	0
Multicast	0	0	0
Broadcast	0	0	0
Bytes	0	0	0
Jumbos	0	0	0
Dropped	0	0	0
Filtered	0	0	0
Pause Frames	0	0	0
L3 Packets	0	0	0
L3 Bytes	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0
Other	0	0	0

Showing information when the interface is currently linked at a downshifted speed:

```

switch(config-if)# show interface 1/1/1
Interface 1/1/1 is up
...
Auto-negotiation is on with downshift active

```

Showing information when the interface is shut down during a VSX split:

```

switch(config-if)# show interface 1/1/1
Interface 1/1/1 is down
Admin state is up
State information: Disabled by VSX
Link state: down for 3 days (since Tue Mar 16 05:20:47 UTC 2021)
Link transitions: 0
Description:
Hardware: Ethernet, MAC Address: 04:09:73:62:90:e7
MTU 1500
Type SFP+DAC3
Full-duplex
qos trust none
Speed 0 Mb/s

```

```

Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: 1502-1505
Rate collection interval: 300 seconds

```

Rate	RX	TX	Total (RX+TX)
Mbps / 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)
Mbps / sec	30196.43	30196.43	60392.85
MPkts / sec	58977.39	58977.40	117954.79
Unicast	0.00	0.00	0.00
Multicast	58977.39	58977.40	117954.79
Broadcast	0.00	0.00	0.00
Utilization %	75.49	75.49	150.98
Statistic	RX	TX	Total (RX+TX)
Packets	4756527649	4756527865	9513055514
Unicast	0	0	0
Multicast	4756527649	4756527865	9513055514
Broadcast	2	0	2
Bytes	304417778668	304417795428	608835574096
Jumbos	0	0	0
Dropped	0	19028847730	19028847730
Pause Frames	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0

```
help: ?, quit: q
```

```
Help for Interface Monitor
h  Toggle human-readable mode
c  Clear interface statistics
Does not apply to rates
Arrows, PgUp, PgDn, Home, End
Navigate interface statistics
Delay: 2
help: ?, quit: q
```

Showing the output for interface 1/1/1 in human-readable format:



In human-readable format, the **< 1** symbol for **Utilization** indicates that the amount of packets is between zero and one. This is true in cases where the number of bytes increases but the number of packets and the **Utilization** value is not displayed even in the normal output, where the human-readable parameter is not included in the command.

```
switch(config-if)# show interface 1/1/1 human-readable
Interface 1/1/1 is up

```

Rate	RX	TX	Total (RX+TX)
Bits / sec	3M	3M	6M
Pkts / sec	316	316	633
Unicast	319	319	638
Multicast	0	0	0
Broadcast	0	0	0
Utilization %	< 1	< 1	< 1

```

Statistic      RX      TX      Total
-----
Packets        577K    577K    1M
Unicast        577K    577K    1M
Multicast       0        51      51
Broadcast       0        15      15
Bytes          744M    745M    1G
Jumbos          0        0        0
Dropped         0        0        0
Filtered        0        0        0
Pause Frames    0        0        0
Errors          0        0        0
CRC/FCS         0        n/a      0
Collision       n/a      0        0
Runts           0        n/a      0
Giants          0        n/a      0

```

Showing information about extended counters:



The output of the `show interface extended` command varies depending on the switch model and configuration.

```
switch(config-if)# show interface 1/1/17 extended
-----
Interface 1/1/17
```

Statistics	Value
Dot1d Tp Port In Frames	547
Dot1d Tp Port Out Frames	608
Dot3 In Pause Frames	0
Dot3 Out Pause Frames	0
Ethernet Stats Broadcast Packets	19
Ethernet Stats Bytes	40162
Ethernet Stats Packets	342
...	
Error-Statistics	Value
Dot1d Base Port MTU Exceeded Discards	0
Dot3 Control In Unknown Opcodes	0
Dot3 Stats Alignment Errors	0
Dot3 Stats FCS Errors	0
Dot3 Stats Frame Too Longs	0
Dot3 Stats Internal Mac Transmit Errors	0
Ethernet RX Oversize Packets	0
...	

Showing interface link-status:

```
switch# show interface link-status
```

Port	Type	Physical Link State	Link Transitions	Last Change
1/1/1	1G-BT	down	0	--
1/1/2	1G-BT	up	1	1 minute ago (Fri Mar 09 12:36:56 UTC 2018)
1/1/3	1G-BT	up	1	1 minute ago (Fri Mar 09 12:36:56 UTC 2018)
1/1/4	--	down	0	--
1/1/5	--	down	0	--

Showing interface loopback 1 link-status:

Port	Type	Physical Link State	Link Transitions	Last Change
loopback1	--	up	--	--

Showing interface 1/1/2-1/1/3 link-status:

Port	Type	Physical Link State	Link Transitions	Last Change
1/1/2	1G-BT	up	1	1 minute ago (Fri Mar 09 12:36:56 UTC 2018)


```
1/1/3          1G-BT          up          1          1 minute ago (Fri Mar 09
12:36:56 UTC 2018)
```

Showing interface link-status:

```
switch# show interface link-status
-----
Port           Type           Physical      Link           Link Flaps      Last
              Link State    Transitions   Ignored        Change
-----
1/1/1          1G-BT          down          0              0              --
1/1/2          1G-BT          up            1              0              1 minute ago
(Fri Mar 09 12:36:56 UTC 2018)
1/1/3          1G-BT          up            1              0              1 minute ago
(Fri Mar 09 12:36:56 UTC 2018)
1/1/4          --             down          0              0              --
1/1/5          --             down          0              0              --
```

Showing state information when interface is blocked:

```
8360(config-if)# show interface 1/1/1

Interface 1/1/1 is up (Blocked)
Admin state is up
State information: Blocked by UDLD
Link state: up for 1 minute (since Mon Jun 10 09:25:27 UTC 2024)
Link transitions: 1
Description:
Persona:
Hardware: Ethernet, MAC Address: 00:fd:45:67:85:91
MTU 1500
Type 10G-LR / 10G SFP+ LR
Full-duplex
qos trust none
Speed 10000 Mb/s
Auto-negotiation is off
Flow-control: off
Error-control: off
VLAN Mode: access
Access VLAN: 1
Rate collection interval: 300 seconds

Rate           RX           TX           Total (RX+TX)
-----
Mbits / sec    0.00         0.00         0.00
KPkts / sec    0.00         0.00         0.00
Unicast        0.00         0.00         0.00
Multicast      0.00         0.00         0.00
Broadcast      0.00         0.00         0.00
Utilization %  0.00         0.00         0.00
Statistic      RX           TX           Total
-----
Packets        15          15          30
Unicast        12          12          24
Multicast       3           3           6
Broadcast       0           0           0
Bytes         1350        1350        2700
Jumbos         0           0           0
Dropped        0           0           0
```

Pause Frames	0	0	0
Errors	0	0	0
CRC/FCS	0	n/a	0
Collision	n/a	0	0
Runts	0	n/a	0
Giants	0	n/a	0

Command History

Release	Modification
10.15	Added state information when port goes into down state.
10.11	Added <code>monitor</code> parameter.
10.10	Added <code>human-readable</code> parameter.
10.07 or earlier	--

Command Information

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

show interface dom

```
show interface [<INTERFACE-ID>] dom [detail] [vsx-peer]
```

Description

Shows diagnostics information and alarm/warning flags for the optical transceivers (SFP, SFP+, QSFP+). This information is known as DOM (Digital Optical Monitoring). DOM information also consists of vendor determined thresholds which trigger high/low alarms and warning flags.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: 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 status: llfc rx	incompatible	0
1/1/10	config: pfc rxtx-1,2 status: none	pending	1234
1/1/12	config: pfc rxtx-1,2 status: none	pending	0
1/1/32:4	config: pfc rxtx-5 status: none		

Showing detailed flow control information with RX flow control enabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rx

Statistics                               RX
-----
Dot3 Pause Frames                       0
```

Showing detailed flow control information with RX flow control enabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rx
Flow-control watchdog: disabled

Statistics                               RX
-----
Dot3 Pause Frames                       0
```

Showing detailed flow control information with RXTX flow control enabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: llfc rxtx

Statistics                               RX                               TX
-----
Dot3 Pause Frames                       0                               0
```

Showing detailed flow control information with PFC enabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
```

Statistics	RX	TX
-----	-----	-----
Priority 0 Pauses	0	0
Priority 1 Pauses	0	0
Priority 2 Pauses	0	0
Priority 3 Pauses	0	0
Priority 4 Pauses	0	0
Priority 5 Pauses	0	0
Priority 6 Pauses	0	0
Priority 7 Pauses	0	0
Total Pause Frames	0	0

Showing detailed flow control information with PFC enabled and flow control watchdog disabled:

```
switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
Flow-control watchdog: disabled
```

Statistics	RX	TX
-----	-----	-----
Priority 0 Pauses	0	0
Priority 1 Pauses	0	0
Priority 2 Pauses	0	0
Priority 3 Pauses	0	0
Priority 4 Pauses	0	0
Priority 5 Pauses	0	0
Priority 6 Pauses	0	0
Priority 7 Pauses	0	0
Total Pause Frames	0	0

```
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
Flow-control watchdog: disabled
```

Statistics	RX	TX
-----	-----	-----
Priority 0 Pauses	0	0
Priority 1 Pauses	0	0
Priority 2 Pauses	0	0
Priority 3 Pauses	0	0
Priority 4 Pauses	0	0
Priority 5 Pauses	0	0
Priority 6 Pauses	0	0
Priority 7 Pauses	0	0
Total Pause Frames	0	0

Showing detailed flow control information with both PFC and flow control watchdog enabled:

```

switch# show interface 1/1/1 flow-control detail
Interface 1/1/1 is up
Admin state is up
Link state: up for 3 minutes (since Thu Apr 07 16:38:02 UTC 2022)
Flow-control: pfc rxtx-4,5
Flow-control watchdog: enabled

Statistics
-----
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 [<IFNAME>|<IFRANGE>] link-diagnostics

Description

Shows information about select link diagnostics, including MAC, PHY, and Transceiver diagnostics.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
link-diagnostics	Shows link diagnostics information.

Examples

Showing interface information for 1/1/12 link diagnostics:

```
switch# show interface 1/1/12 link-diagnostics
```

```
-----
Interface 1/1/12      Current State      Changes      Last Change
-----
Port Status          Waiting for link
Link Down Reason      Local fault

Transceiver
No transceiver        --              0              --
TX Fault              --              0              --
Transceiver error     --              0              --
System error          --              0              --
DOM error             --              0              --
Configuring transceiver --              0              --
Transceiver disabled  --              0              --
Transceiver unsupported --              0              --
MAC and PHY
TX Disabled           --              0              --
Autoneg Incomplete    --              0              --
No Signal Detected     --              0              --
No RX Lock             True             1              22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Remote Fault          --              0              --
```



```

Local Fault          True          1          22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Link State           Down          1          16 seconds ago
(Tue Nov 14 14:30:54 UTC 2023)
switch# show interface 1/1/12 link-diagnostics
-----
Interface 1/1/12      Current State      Changes      Last Change
-----
Port Status          Link up
Link Down Reason      --

Transceiver
No transceiver        --          0          --
TX Fault              --          0          --
Transceiver error     --          0          --
System error          --          0          --
DOM error             --          0          --
Configuring transceiver --          0          --
Transceiver disabled  --          0          --
Transceiver unsupported --          0          --
MAC and PHY
TX Disabled           --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Autoneg Incomplete    --          0          --
No Signal Detected     --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
No RX Lock            --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Remote Fault          --          2          21 seconds
ago (Tue Nov 14 14:30:49 UTC 2023)
Local Fault           --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
  Link State          Up          1          16 seconds
ago (Tue Nov 14 14:30:54 UTC 2023)

```

Showing interface information for 1/1/7-1/1/8 link-diagnostics:

```

switch# show interface 1/1/7-1/1/8 link-diagnostics
-----
Interface 1/1/7      Current State      Changes      Last Change
-----
Port Status          Link up
Link Down Reason      --

Transceiver
No transceiver        --          0          --
TX Fault              --          0          --
Transceiver error     --          0          --
System error          --          0          --
DOM error             --          0          --
Configuring transceiver --          0          --
Transceiver disabled  --          0          --
Transceiver unsupported --          0          --
MAC and PHY
TX Disabled           --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Autoneg Incomplete    --          0          --
No Signal Detected     --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
  No RX Lock          --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)

```

```

Remote Fault          --          2          21 seconds
ago (Tue Nov 14 14:30:49 UTC 2023)
Local Fault          --          2          22 seconds
ago (Tue Nov 14 14:30:48 UTC 2023)
Link State            Up          1          16 seconds
ago (Tue Nov 14 14:30:54 UTC 2023)
-----
Interface 1/1/8      Current State      Changes      Last Change
-----
Port Status          Link up
Link Down Reason      --

Transceiver
No transceiver        --          0          --
TX Fault              --          0          --
Transceiver error      --          0          --
System error          --          0          --
DOM error             --          0          --
Configuring transceiver --          0          --
Transceiver disabled  --          0          --
Transceiver unsupported --          0          --
MAC and PHY
TX Disabled           --          2          22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Autoneg Incomplete    --          0          --
No Signal Detected     --          2          22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
No RX Lock             --          2          22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Remote Fault          --          2          21 seconds ago
(Tue Nov 14 14:30:49 UTC 2023)
Local Fault           --          2          22 seconds ago
(Tue Nov 14 14:30:48 UTC 2023)
Link State            Up          1          16 seconds ago
(Tue Nov 14 14:30:54 UTC 2023)

```

Command History

Release	Modification
10.14	Command introduced.

Command Information

Platforms	Command context	Authority
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 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 P
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	0
1/1/11	0	0	0	0	0	0	0	0	0	0	0	0
1/1/12	0	0	0	0	0	0	0	0	0	0	0	0
...												
1/1/30 - lag1	0	0	0	11271	92	0	0	0	0	51	0	0
1/1/31 - lag2	2360	25	50	2732119	2040	0	0	0	178	1839	0	0
1/1/32 - lag2	0	0	0	11373	93	0	0	0	0	51	0	0
vlan1	0	0	0	0	0	0	0	0	0	0	0	0

Showing statistics of all interfaces with only non-zero statistics:

```
show interface statistics non-zero
```

Interface	RX Bytes	RX Packets	RX Drops	TX Bytes	TX Packets	TX Drops	RX Broadcast	RX Multicast	TX Broadcast	TX Multicast	RX Pause	TX Pause
1/1/1	2727136	1975	0	17796	195	0	82	1788	96	54	0	0
1/1/30 - lag1	0	0	0	11271	92	0	0	0	0	51	0	0
1/1/31 - lag2	2360	25	50	2732119	2040	0	0	0	178	1839	0	0
1/1/32 - lag2	0	0	0	11373	93	0	0	0	0	51	0	0

Showing statistics of all interfaces in the human-readable format:

```
show interface statistics human-readable
```

Interface	RX Bytes	RX Pkts	RX Drops	TX Bytes	TX Pkts	TX Drops	RX Bcast	RX Mcast	TX Bcast	TX Mcast	RX Pause	TX Pause
1/1/1	744M	577K	0	745M	578K	0	0	0	73	287	0	0
1/1/2	474M	367K	0	475M	369K	0	0	0	73	288	0	0
1/1/3	0	0	0	0	0	0	0	0	0	0	0	0

Showing statistics of a single interfaces:

```
show interface 1/1/2 statistics
```

Interface	RX Bytes	RX Packets	RX Drops	TX Bytes	TX Packets	TX Drops	RX Broadcast	RX Multicast	TX Broadcast	TX Multicast	RX Pause	TX Pause
1/1/2	2725080	1931	0	25877	253	0	21	1788	65	55	0	0

Showing statistics of all members of a LAG interface:

```
show interface lag1 statistics
```

Interface	RX Bytes	RX Packets	RX Drops	TX Bytes	TX Packets	TX Drops	RX Broadcast	RX Multicast	TX Broadcast	TX Multicast	RX Pause	TX Pause
1/1/3 - lag1	2424	26	0	2734082	2062	0	0	0	191	1848	0	0
1/1/30 - lag1	0	0	0	12383	100	0	0	0	0	59	0	0
lag1	2424	26	0	2746465	2162	0	0	0	191	1907	0	0

Showing error statistics of all interfaces:

```
show interface error-statistics
```

Interface	RX Errors	TX Errors	Giants	Runts	CRC/FCS	Collisions
1/1/1	190	20	100647	0	0	0
1/1/10	0	0	100	290	7165	949
1/1/11	0	0	0	0	0	0
1/1/12	0	0	0	0	0	0
...						
1/1/30 - lag1	1500	500	45800	0	0	0
1/1/31 - lag2	0	0	11	27	0	0
1/1/32 - lag2	0	0	0	0	6	18

Showing monitor statistics:



The rows and columns of show interface monitor statistics depends on the length of width of the client terminal. The CLI can be navigated using the arrow keys as well as the PageUp, PageDown, Home, and End keys.

```
show interface statistics monitor
```

Interface	RX Bytes	RX Packets >>
1/1/1	3440525421984	53758209526
1/1/2	3440526607008	53758228042
1/1/3	3440527785312	53758246453
1/1/30	3440559671264	53758744653
1/1/31	3440560851680	53758763098
1/1/32	3440562028704	53758781489

help: ?, quit: q

Help for Interface Monitor

f Toggle full statistics
h Toggle human-readable mode
n Toggle non-zero mode
r Toggle rate display

c Clear interface statistics
Does not apply to rates

Arrows, PgUp, PgDn, Home, End
Navigate interface statistics

Delay:2

help: ?, quit: q

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    MYxxxxxxx  1990-3657
1/1/2     SFP+ER*   --        --         --
1/2/1     QSFP+SR4  JH233A    MYxxxxxxx  2005-1234
1/2/2     QSFP+ER4* --        --         --
1/3/1     SFP28DAC3 844477-B21 MYxxxxxxx  77fc-7ce7
* unsupported transceiver
```

Showing detailed transceiver information:

```
switch(conf#) show interface transceiver detailing
Transceiver in 1/1/1
  Interface Name      : 1/1/1
  Type                : SFP+SR
  Connector Type      : LC
  Wavelength          : 850nm
  Transfer Distance   : 0m (SMF), 30m (OM1), 80m (OM2), 300m (OM3)
  Diagnostic Support  : DOM
  Product Number      : J9150A
  Serial Number       : MYxxxxxxx
  Part Number        : 1990-3657

Status
  Temperature        : 47.65C
  Voltage            : 3.31V
  Tx Bias            : 8.40mA
  Rx Power           : 0.08mW, -10.96dBm
  Tx Power           : 0.56mW, -2.49dBm

Recent Alarms :
  Rx power low alarm
  Rx power low warning
Recent Errors :
  Rx loss of signal

Transceiver in 1/1/2
```

```

Interface Name      : 1/1/2
Type               : unknown
Connector Type     : ??
Wavelength         : ??
Transfer Distance  : ??
Diagnostic Support  : ??
Product Number     : ??
Serial Number      : ??
Part Number        : ??

Transceiver in 1/2/1
Interface Name      : 1/2/1
Type               : QSFP+SR4
Connector Type     : MPO
Wavelength         : 850nm
Transfer Distance  : 0m (SMF), 0m (OM1), 0m (OM2), 100m (OM3)
Diagnostic Support  : DOM
Product Number     : JH233A
Serial Number      : MYxxxxxxx
Part Number        : 2005-1234

Status
Temperature : 44.46C
Voltage      : 3.30V

```

Channel#	Tx Bias (mA)	Rx Power (mW/dBm)	Tx Power (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
<i>IFNAME</i>	Specifies the name of an interface on the switch. Use the following format: member/slot/port. Example: 1/3/1
<i>IFRANGE</i>	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
1G-LX          J4859        1/1/33-1/1/34
8x25G-DAC2     S4B39        1/1/2,1/1/4,1/1/6,1/1/8,1/1/10,1/1/12,1/1/14,
              1/1/16,1/1/18,1/1/20,1/1/22,1/1/24,1/1/26,
              1/1/28,1/1/30,1/1/32
QSA28          845970       1/1/1-1/1/32
```

Note: For full product numbers (SKUs) with revision letters, refer to the transceiver guide.

```
switch# show interface supported-transceivers
```

Type	Product Number	Supported Interfaces
100M-FX	J9054	1/10/1-1/10/24,1/12/1-1/12/48
1G-BT	JL747	1/5/49-1/5/52,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48
10G-BT	JL563	1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,1/12/1-1/12/48
10G-BiDi-D	R9X54	1/4/1-1/4/12,1/6/1-1/6/36,1/11/1-1/11/12,1/12/1-1/12/48
10G-SR	J9150	1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/1-1/10/28,1/11/1-1/11/12,1/12/1-1/12/48
10G-SR	JL782	1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12
25G-AOC15	R0Z21	1/6/1-1/6/32
25G-AOC7	R0M45	1/6/1-1/6/32
25G-BiDi-10-U	S1C98	1/4/1-1/4/12,1/5/49-1/5/52,1/6/1-1/6/36,1/5/49-1/5/52,1/6/1-1/6/32,1/7/25-1/7/28,1/8/25-1/8/28,1/9/49-1/9/52,1/10/25-1/10/28,1/12/1-1/12/48
8x50G-DAC2	S4B42	1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12
QSA28	845970	1/4/1-1/4/12,1/6/33-1/6/36,1/11/1-1/11/12

Note: For full product numbers (SKUs) with revision letters, refer to the transceiver guide.

Showing a single interface:

```
switch# show interface 1/1/1 supported-transceivers
```

Type	Product Number	Description
Interface 1/1/1		
10G-BiDi-D @	R9X54	10G BX-D 40km
10G-BiDi-U @	R9X55	10G BX-U 40km
100G-LR4	JL310	100G QSFP28 LR4
100G-SR1.2	S4B44	100G SR1.2 Q28 LC
100G-SR2	S1C93	100G MPO SR2
100G-SR4	JL309	100G QSFP28 SR4
QSA28	845970	--

@ This transceiver is only supported when inserted in a QSA

For full product numbers (SKUs) with revision letters, refer to the Transceiver guide.

Showing a range of interfaces:

```
switch# show interface 1/1/1-1/1/2 supported-transceivers
```

Type	Product Number	Description

Interface 1/1/1		
10G-BiDi-D @	R9X54	10G BX-D 40km
10G-BiDi-U @	R9X55	10G BX-U 40km
10G-ER @	S2P32	10G SFP+ ER
100G-SR2	S1C93	100G MPO SR2
100G-SR4	JL309	100G QSFP28 SR4
QSA28	845970	--
Interface 1/1/2		
10G-BiDi-D @	R9X54	10G BX-D 40km
10G-BiDi-U @	R9X55	10G BX-U 40km
10G-ER @	S2P32	10G SFP+ ER
25G-BiDi-10-D @	S1C96	25G LC BiDi 10km-D
25G-SR @	S2P33	25G SFP28 SR
40G-eSR4	JH233	QSFP+ eSR4
100G-BiDi	845972	--
100G-SR4	JL309	100G QSFP28 SR4
QSA28	845970	--
@ This transceiver is only supported when inserted in a QSA For full product numbers (SKUs) with revision letters, refer to the Transceiver guide.		

Showing a chassis switch with multiple line modules:

switch# show interface supported-transceivers		

Type	Product Number	Supported Interfaces

100M-FX	J9054	1/10/1-1/10/24,1/12/1-1/12/48
1G-BT	JL747	1/5/49-1/5/52,1/7/25-1/7/28,1/8/25-1/8/28, 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 Number	Supported 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.

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.

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.

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.

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.

The splittable ports for all models are shown in the table below:

Model	Description	Port info
8400X modules - JL365A - JL366A	8400X 8p 40G QSFP+ Adv Module 8400X 6p 40G/100G QSFP28 Adv Module	1-8 (40G) 1-6 Only capable of 40G split into 4 x 10G JL366A modules do not have 25G MACs to support split 100G
8400X modules		

Model	Description	Port info
▪ JL365A ▪ JL366A	8400X 8p 40G QSFP+ Adv Mod 8400X 6p 40G/100G QSFP28 Adv Mod	1-8 (40G) 1-6 Only capable of 40G split into 4 x 10G JL366A modules do not have 25G MACs to support split 100G

Examples

Splitting an interface:

```
switch(config-if)# interface 1/1/1
switch(config-if)# split
```

This command will disable the specified port, clear its configuration, and split it into multiple interfaces. The split interfaces will not be available until the next system or line module reboot.

Continue (y/n)? y

```
switch(config-if)# show interface brief
```

```
-----
--
Port      Native Mode   Type           Enabled Status Reason           Speed
Desc      VLAN
-----
--
1/1/1:1 --      routed QSFP+DA3x4 yes    down    Split reboot pending --  --
1/1/1:2 --      routed QSFP+DA3x4 yes    down    Split reboot pending --  --
1/1/1:3 --      routed QSFP+DA3x4 yes    down    Split reboot pending --  --
1/1/1:4 --      routed QSFP+DA3x4 yes    down    Split reboot pending --  --
```

Unsplitting a port on a switch that requires 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. The port will not be available until the next system or line module reboot.

Continue (y/n)? y

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config-if	Administrators or local user group members with execution rights for this command.

system interface-group

```
system interface-group <GROUP> line-module <SLOT-ID> speed <SPEED>
no system interface-group <GROUP> line-module <SLOT-ID> 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 or 25g) for a group. Default is 25g (see the Transceiver Guide for further detail). On HPE Aruba Networking 8400 Switch Series: 10g allows 1Gbps or 10Gbps transceivers only. 25g allows 25Gbps transceivers only.
<SLOT-ID>	Specifies the slot ID of the line module.

Examples

Configuring interface group 1 on line-module 1/1 to allow 10Gbps and slower transceivers:

```
switch(config)# system interface-group 1 line-module 1/1 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
10.09.0002	Command introduced on 6400 and 8400 Switch series.

Command Information

Platforms	Command context	Authority
8400	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

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
<code><PROTOCOL></code>	Specifies the protocol to configure. ▪ all: Selects the source for all protocols covered by this command. ▪ central: Selects HPE Aruba Networking Central. ▪ dhcp_relay: Selects DHCP relay. When you configure a dhcp_relay source interface, you must also enable DHCP relay Option 82 using the dhcp-relay option 82 source-interface command. ▪ dns: Selects DNS. ▪ http: Selects HTTP. ▪ ntp: Selects NTP. ▪ radius: Selects RADIUS. ▪ sflow: Selects sFlow. ▪ sftp-scp: Selects SFTP and SCP. ▪ ssh-client: Selects SSH Client. ▪ syslog: Selects the source for syslog packets.

Parameter	Description
	▪ tacacs: Selects the source for TACACS packets. ▪ tftp: Selects TFTP.
<IFNAME>	Specifies the interface name.
<IP-ADDR>	Specifies the IPv4 address.
vrf <VRF-NAME>	Specifies the VRF name.

Examples

Configuring IPv4 source-interface interface 1/1/1 to use for the TFTP protocol:

```
switch(config)# ip source-interface tftp interface 1/1/1
```

Configuring IPv4 source-interface interface 1/1/2 to use for the TFTP protocol on VRF **green**:

```
switch(config)# ip source-interface tftp interface 1/1/2 vrf green
```

Removing IPv4 source-interface 1/1/1 configuration for the TFTP protocol:

```
switch(config)# no ip source-interface tftp interface 1/1/1
```

Removing source-interface interface 1/1/2 configuration for TFTP protocol on VRF **green**:

```
switch(config)# no ip source-interface tftp interface 1/1/2 vrf green
```

Configuring source-interface IPv4 10.1.1.1 to use for the TFTP protocol:

```
switch(config)# ip source-interface tftp 10.1.1.1
```

Configuring source-interface IPv4 10.1.1.2 to use for the TFTP protocol on VRF **green**:

```
switch(config)# ip source-interface tftp 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1 configuration for the TFTP protocol:

```
switch(config)# no ip source-interface tftp 10.1.1.1
```

Removing source-interface IPv4 10.1.1.2 configuration for TFTP protocol on VRF **green**:

```
switch(config)# no ip source-interface tftp 10.1.1.2 vrf green
```

Configuring source-interface IPv4 10.1.1.1 to use for the DNS protocol:

```
switch(config)# ip source-interface dns 10.1.1.1
```

Configuring source-interface IPv4 10.1.1.2 to use for the DNS protocol on VRF **green**:

```
switch(config)# ip source-interface dns 10.1.1.2 vrf green
```

Removing source-interface IPv4 10.1.1.1 configuration for the DNS protocol:

```
switch(config)# no ip source-interface tftp 10.1.1.1
```

Removing source-interface IPv4 10.1.1.2 configuration for the DNS protocol on VRF **green**:

```
switch(config)# no ip source-interface dns 10.1.1.2 vrf green
```

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.

Parameter	Description
	▪ http: Selects HTTP. ▪ ntp: Selects NTP. ▪ radius: Selects RADIUS. ▪ sflow: Selects sFlow. ▪ sftp-scp: Selects SFTP and SCP. ▪ ssh-client: Selects SSH Client. ▪ syslog: Selects the source for syslog packets. ▪ tacacs: Selects the source for TACACS packets. ▪ tftp: Selects TFTP.
<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
<i><PROTOCOL></i>	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 relay. dns Shows the source interface configuration for DNS. http Shows the source interface configuration for HTTP. ntp Shows the source interface configuration for NTP. radius Shows the source interface configuration for radius. sflow Shows the source interface configuration for sFlow. sftp-scp

Parameter	Description
	Shows source interface configuration for SFTP and SCP. ssh-client
	Shows source interface configuration for SSH Client. syslog
	Shows the source interface configuration for syslog. tacacs
	Shows the source interface configuration for TACACS. tftp
	Shows the source interface configuration for TFTP.
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Shows the source interface configuration for all VRFs.

Examples

Displaying all source-interface protocol configurations for VRF red:

```
switch# show ip source-interface all vrf red
Source-interface Configuration Information
-----
Protocol      Src-Interface      Src-IP              VRF
-----
all           1/1/1              red
```

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
```

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
```

Command History

Release	Modification
10.12.1000	Added <code>central</code> , <code>sftp-scp</code> , and <code>ssh-client</code> parameters.
10.07 or earlier	--

Command Information

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

show ipv6 source-interface

```
show ipv6 source-interface <PROTOCOL> [detail] [vrf <VRF-NAME> | all-vrfs]
```

Description

Displays the IPV6 source interface information configured in the router for all VRFs or a specific VRF. If a VRF is not specified, the default is displayed.

Parameter	Description
<code><PROTOCOL></code>	Specifies the protocol to show. <code>all</code> Shows the source interface configuration for all other protocols. <code>central</code> Shows the source interface configuration for HPE Aruba Networking Central. <code>dhcp_relay</code> Shows the source interface configuration for DHCP relay. <code>dns</code> Shows the source interface configuration for DNS. <code>http</code> Shows the source interface configuration for HTTP. <code>ntp</code> Shows the source interface configuration for NTP. <code>radius</code> Shows the source interface configuration for radius. <code>sflow</code> Shows the source interface configuration for sFlow. <code>sftp-scp</code> Shows source interface configuration for SFTP and SCP. <code>ssh-client</code> Shows source interface configuration for SSH Client. <code>syslog</code> Shows the source interface configuration for syslog. <code>tacacs</code>

Parameter	Description
	Shows the source interface configuration for TACACS. <code>tftp</code> Shows the source interface configuration for TFTP.
<code>vrf <VRF-NAME></code>	Specifies the VRF name.
<code>all-vrfs</code>	Shows the source interface configuration for all 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#
```

Command History

Release	Modification
10.13	Added the <code>dns</code> protocol parameter.
10.12.1000	Added <code>central</code> , <code>sftp-scp</code> , and <code>ssh-client</code> parameters.
10.07 or earlier	--

Command Information

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

show running-config

`show running-config`

Description

Displays the current running configuration.

Examples

Displaying the running configuration (only items of interest to source interface selection are shown in this example output command):



HPA 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.

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.

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: Ejq2OIa3z3lSGvmK3gyWag==" \
-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
<code><TIME-LAPSE-INTERVAL></code>	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 j1363a
!
!
!
!
!
!
!
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 j1363a
!
!
!
!
!
!
!
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
<code><NEW-CHECKPOINT-NAME></code>	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
<code><CHECKPOINT-NAME></code>	Specifies a checkpoint name.
<code>startup-config</code>	Specifies the startup configuration.

Examples

Applying a checkpoint named **ckpt1** to the running configuration:

```
switch# checkpoint rollback ckpt1
Success
```

Applying a startup checkpoint to the running configuration:

```
switch# checkpoint rollback startup-config
Success
```

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: <code>usb:/<FILE></code> 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 <code>CPC</code> 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
<code><REMOTE-URL></code>	Specifies a remote file with the following syntax: TFTP format: <pre>tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME></pre> SFTP format: <pre>sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME></pre> SCP format: <pre>scp://USER@{IP HOST}[:PORT]/FILE</pre>
<code>startup-config</code>	Indicates that the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration.
<code>running-config</code>	Indicates that the running configuration receives the copied checkpoint configuration.
<code>overwrite</code>	By default, the CLI configuration contained in the copied file is applied on top of the running-config, so the CLI command does not clear the running-config before applying the CLI commands. In the event that a particular CLI command fails then the failure is logged in event logs and the next line in CLI configuration is processed. When you include the overwrite parameter, the configuration is only applied to the running-config if <i>all</i> the commands succeeded without errors. If there are any errors during the copy process, the existing running-config will remain intact. You can then inspect the event logs to check and fix the errors and retry the operation. If more than 20 errors are present, the operation stops processing any further commands. The event logs will display only those errors processed up to that point.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.

Usage

The switch copies only certain file types. The format of the file is automatically detected from contents of the file. The **startup-config** option only supports the JSON file format and checkpoints, but the **running-config** option supports the JSON and CLI file formats and checkpoints.

When a file of the CLI format is copied, it overwrites the running configuration. The CLI command does not clear the running configuration before applying the CLI commands. All of the CLI commands in the file are applied line-by-line. If a particular CLI command fails, the switch logs the failure and it continues to the next line in the CLI configuration. The event log (**show events -d hpe-config**) provides information as to which command failed.

Examples

Copying a JSON format file to the running configuration:

```
switch# copy tftp://192.168.1.10/runjson running-config  
##### 100.0%
```



```
Configuration may take several minutes to complete according to configuration file
size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Success
```

Copying a CLI format file to the running configuration with an error in the file:

```
switch# copy tftp://192.168.1.10/runcli running-config
##### 100.0%
Configuration may take several minutes to complete according to configuration file
size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Some of the configuration lines from the file were NOT applied. Use 'show
events -d hpe-config' for more info.
##### 100.0%
Configuration may take several minutes to complete according to configuration file
size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Some of the configuration lines from the file were NOT applied. Use 'show
events -d hpe-config' for more info.
```

Copying a CLI format file to the startup configuration:

```
switch# copy tftp://192.168.1.10/startjson startup-config
##### 100.0%
100.0%
Success
```

Copying an unsupported file format to the startup configuration:

```
switch# copy tftp://192.168.1.10/startfile startup-config
##### 100.0%
100.0%
unsupported file format
```

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.
<code>startup-config</code>	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.
<code>checkpoint <CHECKPOINT-NAME></code>	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 <checkpoint-name>
  core-dump all|daemon|dsm|kernel
  startup-config
  all
```

Description

Deletes an existing checkpoint, startup configuration, or core-dump.

Parameter	Description
<code>checkpoint <CHECKPOINT-NAME></code>	Specifies the name of a checkpoint.
<code>core-dump</code> <code>all daemon <daemon-name></code> <code> kernel</code>	Erase one of the following sets of core-dump files: - all: Erase all core-dump files. - daemon <daemon-name>: Erase daemon core-dump files. - kernel: Erase the kernel core-dump.
<code>startup-config</code>	Specifies the startup configuration.
<code>all</code>	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
10.07 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
AQBapQjwipecbv36io0jFfde7ZzrHckncallD+3n8XFTZKQdmYgAAADetYOeHSme93xzdD0uz6Vr9K1+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 ending date 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 <code>show checkpoint list date <START-DATE> <END-DATE></code> is replaced with <code>show checkpoint date <START-DATE> <END-DATE></code>
10.07 or earlier	--

Command Information

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

show running-config hash

`show running-config hash [cli | json]`

Description

Shows the running-config checkpoint hash, calculated with the SHA-256 algorithm. When the output format is not specified, the CLI format is used. This enables you to determine whether there has been a configuration change since a previous hash was calculated.

Parameter	Description
[cli json]	Selects either the CLI or JSON format.

Examples

Showing the running-config checkpoint SHA-256 hash in CLI format:

```
switch# show running-config hash cli
Calculating the hash: [Success]

SHA-256 hash of the config in CLI format:

8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62aa1d715075b89e

This hash is only valid for comparison to a baseline hash if the configuration has
not been explicitly changed (such as with a CLI command, REST operation, etc.)
or implicitly changed (such as by changing a hardware module, upgrading the
SW version, etc.).
```

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 fabric-module

boot fabric-module <SLOT-ID>

Description

Reboots the specified fabric module.

Parameter	Description
<SLOT-ID>	Specifies the member and slot of the module in the format member/slot . For example, to specify the module in member 1 slot 3, enter 1/3 .

Usage

The **boot fabric-module** command reboots the specified fabric module. Traffic performance is affected while the module is down.

If the specified module is the only fabric module in an up state, rebooting that module stops traffic switching between line modules and the line modules power down. The line modules power up when one fabric module returns to an up state.

This command is valid for fabric modules only.

Examples

Rebooting the fabric module in slot **1/3** when auto-confirm is not enabled:

```
switch# boot fabric-module 1/3
This command will reboot the specified fabric module. Traffic performance may
be affected while the module is down. Rebooting the last fabric module will
stop traffic switching between line modules.
Do you want to continue (y/n)? y

switch#
```

Rebooting the fabric module in slot **1/1** when auto-confirm is enabled:

```
switch# boot fabric-module 1/3
This command will reboot the specified fabric module. Traffic performance may
be affected while the module is down. Rebooting the last fabric module will
stop traffic switching between line modules.
Do you want to continue (y/n) y (auto-confirm)

switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Manager (#)	Administrators or local user group members with execution rights for this command.

boot line-module

boot line-module <SLOT-ID>

Description

Reboots the specified line module.

Parameter	Description
<SLOT-ID>	Specifies the member and slot of the module in the format member/slot . For example, to specify the module in member 1 slot 3, enter 1/3 .

Usage

Reboots the specified line module. Any traffic for the switch passing through the affected module (SSH, TELNET, and SNMP) is interrupted. It can take up to 2 minutes to reboot the module. During that time, you can monitor progress by viewing the event log.

This command is valid for line modules only.

Examples

Reloading the module in slot 1/1:


```
switch# boot line-module 1/1
This command will reboot the specified line module and interfaces on this
module will not send or receive packets while the module is down. Any
traffic passing through the line module will be interrupted. Management
sessions connected through the line module will be affected. It might take
up to 2 minutes to complete rebooting the module. During that time, you can
monitor progress by viewing the event log.
Do you want to continue (y/n)? y
switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Manager (#)	Administrators or local user group members with execution rights for this command.

boot management-module

```
boot management-module {active | standby | <SLOT-ID>}
```

Description

Reboots the specified management module. Choose the management module to reboot by role (active or standby) or by slot number.

Parameter	Description
<i>active</i>	Selects the active management module.
<i>standby</i>	Selects the standby management module.
<i><SLOT-ID></i>	Specifies the member and slot of the management module in the format member/slot . For example, to specify the module in member 1 slot 5, enter 1/5 .

Usage

This command reboots a single management module in a chassis. Choose the management module to reboot by role (active or standby) or by slot number.

You can use the **show images** command to show information about the primary and secondary system images.

If you reboot the active management module and the standby management module is available, the active management module reboots and the standby management module becomes the active management module.

If you reboot the active management module and the standby management module is not available, you are warned, you are prompted to save the configuration, and you are prompted to confirm the operation.

If you reboot the standby management module, the standby management module reboots and remains the standby management module.

If you attempt to reboot a management module that is not available, the **boot** command is aborted.

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** command is aborted.



Hewlett Packard Enterprise recommends that you use the **boot management-module** command instead of pressing the module reset button to reboot a management module because if you are rebooting the only available management module, the **boot management-module** command enables you to save the configuration, cancel the reboot, or both.

Examples

Rebooting the active management module when the standby management module is available:

```
switch# boot management-module active
The management-module in slot 1/5 is going down for reboot now.
```

Rebooting the active management module when the standby management module is not available:

```
switch# boot management-module 1/5
The management module in slot 1/5 is currently active and no
standby management module was found.
This will reboot the entire switch.

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.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Manager (#)	Administrators or local user group members with execution rights for this command.

boot management-module (recovery console)

`boot management-module {local|remote}`

Description

Reboots the specified management module by specified location (local or remote).

Parameter	Description
<code><local></code>	Reboots the local management module.
<code><remote></code>	Reboots the remote management module.

Usage

This command reboots a single management module in a chassis. Choose the management module to reboot by role (active or standby) or by slot number.

You can use the **show images** command to show information about the primary and secondary system images.

If you reboot the active management module and the standby management module is available, the active management module reboots and the standby management module becomes the active management module.

If you reboot the active management module and the standby management module is not available, you are warned, you are prompted to save the configuration, and you are prompted to confirm the operation.

If you reboot the standby management module, the standby management module reboots and remains the standby management module.

If you attempt to reboot a management module that is not available, the **boot** command is aborted.

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** command is aborted.



Hewlett Packard Enterprise recommends that you use the **boot management-module** command instead of pressing the module reset button to reboot a management module because if you are rebooting the only available management module, the **boot management-module** command enables you to save the configuration, cancel the reboot, or both.

Examples

Booting a remote management module:

```
switch# boot management-module remote
There is no other management module installed.
Aborting.
switch#
```

Command History

Release	Modification
10.12	Command introduced.

Command Information

Platforms	Command context	Authority
8400	Manager (#)	Administrators or local user group members with execution rights for this command.

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

Parameter	Description
	sets the configured default operating system image to primary for future reboots.
<code>secondary</code>	Selects the secondary operating system image for this reboot and sets the configured default operating system image to secondary for future reboots.
<code>serviceos</code>	Selects the service operating system for this reboot. Does not change the configured default operating system image. The service operating system acts as a standalone bootloader and recovery OS for switches running the AOS-CX operating system and is used in rare cases when troubleshooting a switch.

Usage

This command reboots the entire system. If you do not select one of the optional parameters, the system reboots from the configured default boot image.

You can use the **show images** command to show information about the primary and secondary system images.

Choosing one of the optional parameters affects the setting for the default boot image:

- If you select the **primary** or **secondary** optional parameter, that image becomes the configured default boot image for future system reboots. The command fails if the switch is not able to set the operating system image to the image you selected.

You can use the **boot set-default** command to change the configured default operating system image.

- If you select **serviceos** as the optional parameter, the configured default boot image remains the same, and the system reboots all management modules with the service operating system.

If the configuration of the switch has changed since the last reboot, when you execute the **boot system** command you are prompted to save the configuration and you are prompted to confirm the reboot operation.

Saving the configuration is not required. However, if you attempt to save the configuration and there is an error during the save operation, the **boot system** command is aborted.

Examples

Rebooting the system from the configured default operating system image:

```
switch# boot system
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.
The system is going down for reboot.
```

Rebooting the system from the secondary operating system image, setting the secondary operating system image as the configured default boot image:

```
switch# boot system secondary
Default boot image set to secondary.

Do you want to save the current configuration (y/n)? n

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? y
The system is going down for reboot.
```

Canceling a system reboot:

```
switch# boot system

Do you want to save the current configuration (y/n)? n

This will reboot the entire switch and render it unavailable
until the process is complete.
Continue (y/n)? n
Reboot aborted.
switch#
```

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.

For switches that support line modules (such as 8400 switch series) including the **all** parameter displays information for the active management module and all available line modules.



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. For switches that support line modules, including this parameter displays information for and all available line modules.
vsf member <1-10>	Optional. Display boot history for the specified VSF member

Usage

This command displays the boot-index, boot-ID, and up time in seconds for the current boot. If there is a previous boot, it displays boot-index, boot-ID, reboot time (based on the time zone configured in the system) and reboot reasons. Previous boot information is displayed in reverse chronological order.

The output of this command includes the following information:

Parameter	Description
Index	The position of the boot in the history file. Range: 0 to 3.
Boot ID	A unique ID for the boot . A system-generated 128-bit string.
Current Boot, up for <time>	For the current boot, the show boot-history command shows the number of seconds the module has been running on the current software.
<Timestamp>: boot reason	For previous boot operations, the show boot-history command shows the time at which the operation occurred and the reason for the boot. The reason for the boot is one of the following values: ▪ <DAEMON-NAME> crash: The daemon identified by <DAEMON-NAME> caused the module to boot. ▪ Kernel crash: The operating system software associated with the module caused the module to boot. ▪ Uncontrolled reboot: The reason for the reboot is not known. ▪ Reboot requested through database: The reboot occurred because of a request made through the CLI or other API.

Examples

Showing the boot history of the active management module:

```
switch# show boot-history
Management module
=====

Index : 2
Boot ID : c34a2c2499004a02bbeeff4992e1fdbd
Current Boot, up for 1 days 13 hrs 13 mins 27 secs
```

```

Index : 1
Boot ID : bfba9bc486304e57904ac717a0ccbdcd
02 Sep 23 02:55:33 : CPU request reset with 0x20201, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:55:33 : Switch boot count is 2

Index : 0
Boot ID : a88a71b7ca9a4574af7e3b811ddfdc7e
02 Sep 23 02:49:26 : Reboot requested by user, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:50:02 : Switch boot count is 1

Index : 3
Boot ID : f00ba10c8c44457f83fee303d014a89a
25 Aug 23 10:27:42 : Power on reset with 0x1, Version: FL.10.14.0000-1465-
g9df95249d06b0~dirty
25 Aug 23 10:28:18 : Switch boot count is 3
25 Aug 23 10:29:02 : Primary overtemperature fault detected with 0x2 in PSU 1/1

```

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. 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:

Parameter	Description
	<pre>tftp://<IP-ADDR>[:<PORT-NUM>] [;blocksize=<Value>]/<FILENAME></pre> SFTP format: <pre>sftp://<USERNAME>@<IP-ADDR> [:<PORT-NUM>]/<FILENAME></pre> SCP format: <pre>scp://USER@{IP HOST}[:PORT]/FILE</pre>
<code>{hot-patch primary secondary}</code>	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.
<code>vrf <VRF-NAME></code>	Specifies the name of a VRF. Default: default.

TFTP usage

To specify a URL with:

- an IPv4 address: **tftp://192.0.2.1/a.txt**
- an IPv6 address: **tftp://[2000::2]/a.txt**
- a hostname: **tftp://hpe.com/a.txt**

To specify TFTP with:

- the port number of the server in the URL: **tftp://192.0.2.1:12/a.txt**
- the blocksize in the URL: **tftp://192.0.2.1;blocksize=1462/a.txt**

The valid blocksize range is 8 to 65464.

- the port number of the server and blocksize in the URL: **tftp://192.0.2.1:12;blocksize=1462/a.txt**

To specify a file in a directory of URL: **tftp://192.0.2.1/dir/a.txt**

SFTP usage

To specify:

- A URL with an IPv4 address: **sftp://user@192.0.2.1/a.txt**
- A URL with an IPv6 address: **sftp://user@[2000::2]/a.txt**
- A URL with a hostname: **sftp://user@hpe.com/a.txt**
- SFTP port number of a server in the URL: **sftp://user@192.0.2.1:12/a.txt**
- A file in a directory of URL: **sftp://user@192.0.2.1/dir/a.txt**
- To specify a file with absolute path in the URL: **sftp://user@192.0.2.1/home/user/a.txt**

SCP Usage

To specify:

- A username with an IP address: **scp://user@192.0.2.1:12/a.txt**
- A username with a remote host: **scp://user@hpe.com/a.txt**

Examples

TFTP download for a hot-patch:

```
switch# copy tftp://192.168.1.1/FL.10.12.0001-0002.patch hot-patch vrf vrf1

Fetching /users/swuser/FL.10.10.0001-0002.patch to hotpatch.dnld.uE2YT1
FL.10.12.0001-0002.patch                      100%   62KB   12.4MB/s   00:00

Verifying and writing hot-patch...
```

TFTP download for primary software image:

```
switch# copy tftp://192.10.12.0/FL_10_12_0001.swi primary
The primary image will be deleted.

Continue (y/n)? y
##### 100.0%
Verifying and writing system firmware...
```

SFTP download:

```
switch# copy sftp://swuser@192.10.12.0/FL_10_12_0001.swi primary
The primary image will be deleted.

Continue (y/n)? y
The authenticity of host '192.10.12.0 (192.10.12.0)' can't be established.
ECDSA key fingerprint is SHA256:L64khLwlyLgXlARKRmiwcAAK8oRaQ8C0oWP+PkGBXHY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.10.12.0' (ECDSA) to the list of known hosts.
swuser@192.10.12.0's password:
Connected to 192.10.12.0.
Fetching /users/swuser/ss.10.00.0002.swi to ss.10.00.0002.swi.dnld
/users/swuser/ss.10.00.0002.swi                100%  179MB  25.6MB/s   00:07
Verifying and writing system firmware...
```

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:MyIlxbdKnehYut0NLfL69gDpNzCmZqBVvBaRR46m7o8.
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
<code>apply <name.patch></code>	Apply the specified hot-patch image to a standalone switch or VSF stack. AOS-CX hot-patch software images can be obtained from HPE Aruba Networking customer support, and are identified with a .patch extension.
<code>remove <name.patch></code>	Disables the hot-patch image and removes the patch from the switch. This removal will also disable the patch. Once removed, a hot-patch must be downloaded again in order to be applied.

Usage

A hot-patch can be downloaded from a remote server onto a switch then applied without rebooting the switch. When the hot-patch is disabled, the hot-patch will still remain on the system. The disabled hot-patch can be removed from the system without the need for a reboot of the system.

If a checkpoint configuration that does not contain a hot-patch is restored to a running configuration that does have a hot-patch, the patch is not deleted, it remains as not applied but is present in the device memory.

Examples

```
switch(config)# hot-patch apply FL_10_12_0001-0002.patch
```

Related Commands

Command	Description
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
8400	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
8400	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
8400	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.

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.

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 address 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 obtaining 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
```

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.

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

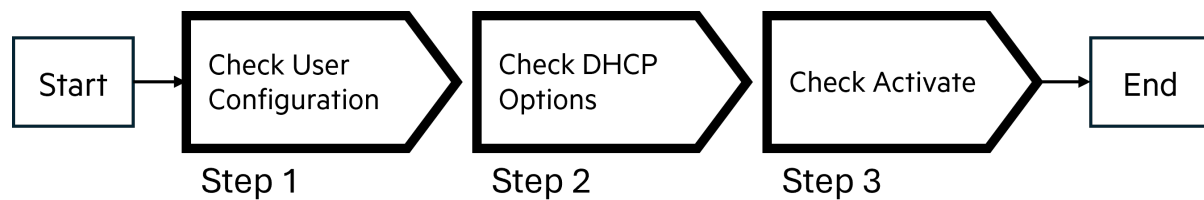
Scenario: Central location discovery

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 Associated Applications	Cert Status	EST Status
----- -----	-----	-----
device-identity none	installed	n/a

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.

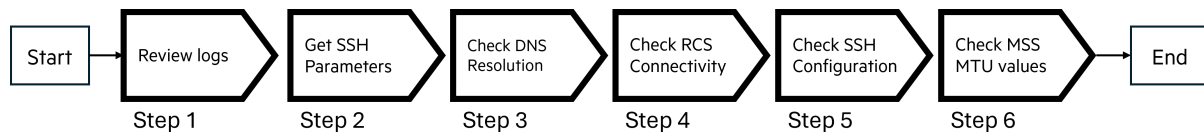
Prerequisites

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:U2DN6AjUh24D475uVopixlihd1nTX7/5zT9P764VhDE
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	

Parameter	Example Value	Notes
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
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

Algorithm	RCS Support
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

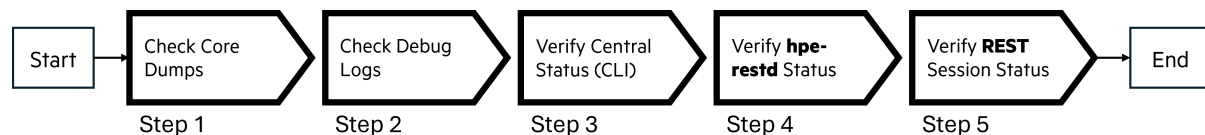
The switch experiences delayed disconnection from Central or the hpe-restd service becomes unresponsive during a disconnection event. This may occur during:

- 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

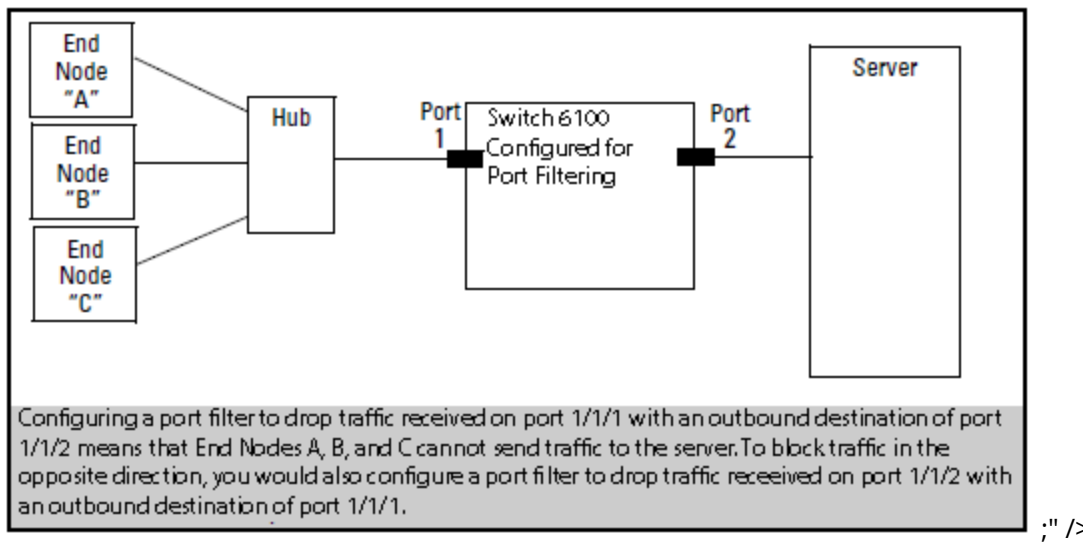
Feature	Reason
Zero Touch Provisioning	Used to receive the Central location via DHCP options when the switch boots
Source interface selection	Used to define the outgoing interface from which the connection to Central and/or Activate is established

Chapter 10

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*



Port filtering commands

The Domain Name System (DNS) is the Internet protocol for mapping domain names or hostnames into 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
<code>list <DOMAIN-NAME></code>	Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.

Examples

This example defines a list with two entries: **domain1.com** and **domain2.com**.

```
switch(config)# ip dns domain-list domain1.com  
switch(config)# ip dns domain-list domain2.com
```

This example 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
<code><DOMAIN-NAME></code>	Specifies the domain name to append to DNS requests. Length: 1 to 256 characters.
<code>vrf <VRF-NAME></code>	Specifies a VRF name. Default: default.

Examples

Setting the default domain name to `domain.com`:

```
switch(config)# ip dns domain-name domain.com
```

Removing the default domain name `domain.com`:

```
switch(config)# no ip dns domain-name domain.com
```

Command History

Release	Modification
10.07 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
<code><IP-ADDR></code>	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.
<code>vrf <VRF-NAME></code>	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	<code>config</code>	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
<code>vrf <VRF-NAME></code>	Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.

Usage

DNS client arbitration on the MGMT interface on a MGMT VRF can be updated via three different methods.

1. Using the **domain-name <name>** or **nameservers <servers>** commands in the command-line interface.
2. Using the **ip dns domain-name <DOMAIN-NAME> vrf MGMT** or **ip dns server-address <SERVER> vrf MGMT** commands in the command-line interface.
3. Using the **ip dhcp** command in the command-line interface (dynamic entries).

AOS-CX gives the following priority levels to the these three update methods.

- Priority 1 - standalone CLI configuration
- Priority 2 - static ip dns configuration
- Priority 3 - Dynamic config

Examples

These examples define DNS settings and then show how they are displayed with the **show ip dns** command.

```
switch(config)# ip dns domain-name domain.com
switch(config)# ip dns domain-list domain5.com
switch(config)# ip dns domain-list domain8.com
switch(config)# ip dns server-address 4.4.4.4
switch(config)# ip dns server-address 6.6.6.6
switch(config)# ip dns host host3 5.5.5.5
switch(config)# ip dns host host2 2.2.2.2
switch(config)# ip dns host host3 c::12
switch(config)# ip dns domain-name reddomain.com vrf red
switch(config)# ip dns domain-list reddomain5.com vrf red
switch(config)# ip dns domain-list reddomain8.com vrf red
switch(config)# ip dns server-address 4.4.4.5 vrf red
switch(config)# ip dns server-address 6.6.6.7 vrf red
switch(config)# ip dns host host3 5.5.5.6 vrf red
switch(config)# ip dns host host2 2.2.2.3 vrf red
switch(config)# ip dns host host3 c::13 vrf red
switch# show ip dns
VRF Name : default

Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6

Host Name      Address
-----
host2          2.2.2.2
host3          5.5.5.5
host3          c::12
VRF Name : red
```

```
Domain Name : reddomain.com
DNS Domain list : reddomain5.com, reddomain8.com
Name Server(s) : 4.4.4.5, 6.6.6.7
```

Host Name	Address
host2	2.2.2.3
host3	5.5.5.6
host3	c::13

```
switch(config)# ip dns domain-name domain.com vrf red
switch(config)# ip dns domain-list domain5.com vrf red
switch(config)# ip dns domain-list domain8.com vrf red
switch(config)# ip dns server-address 4.4.4.4 vrf red
switch(config)# ip dns server-address 6.6.6.6 vrf red
switch(config)# ip dns host host3 5.5.5.5 vrf red
switch(config)# no ip dns host host2 2.2.2.2 vrf red
switch(config)# ip dns host host3 c::12 vrf red
```

```
switch# show ip dns vrf red
VRF Name : red
```

```
Domain Name : domain.com
DNS Domain list : domain5.com, domain8.com
Name Server(s) : 4.4.4.4, 6.6.6.6
```

Host Name	Address
host3	5.5.5.5
host3	c::12

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.

The switch provides support for LLDP and CDP to enable automatic discovery and configuration of other devices on the network.

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 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. Range 1-4094.

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
<code>select-tlv <TLV-NAME></code>	Specifies the TLV name to send. The following TLV names are supported: ▪ management-address: Selection is based on priority in the following list (for example if first TLV name isn't selected, the next will be, progressing through this list until a selection is made): 1. IPv4 or IPV6 management address. 2. IP address of the lowest configured loopback interface. 3. If layer 3, then the route-only port IP address. 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
<code>ip <X.X.X.X></code>	Specify an IP address in IPv4 format (X.X.X.X), where X is a decimal number from 0 to 255.
<code>ipv6 <X:X::X:X></code>	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
8400	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
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
8400	Manager (#)	Operators 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 BASE_TFD
Neighbor MAU type : 1000 BASE_TFD

```

```

-----
Port : 1/1/47
Neighbor Entries : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : 6300
Neighbor Chassis-Description : hpe_anw ...
Neighbor Chassis-ID : 38:11:17:1a:d5:00
Neighbor Management-Address : 38:11:17:1a:d5:00
Chassis 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
8400	Manager (#)	Operators 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
8400	Manager (#)	Operators 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
```

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 13

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 the TFTP 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 file 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 file is deleted from the USB device. This message may also display in the event of an unknown error.



In the case of reconnection, connect with a main or alternative location to the COP instance as a user. The current connection is shown in the **Central location** field.

Scenario 1: If the location the device is currently connected on is updated, the system reconnects in order to connect with the new location.

Scenario 2: If the location in which the device is not currently connected on is updated, the DUT does not go through the reconnection process.

Examples

Showing switch image and config download from an IPv4 TFTP server in progress after receiving ZTP options:

```
switch# show ztp information
TFTP Server                : 10.0.0.2
Image File                 : TL_10_02_0001.swi
Configuration File         : ztp.cfg
ZTP Status                 : In-progress - Image download and verification
HPE ANW Central Location  : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision           : Enabled
HTTP Proxy Location       : NA
```

Showing switch image download failure from an IPv4 TFTP server because the server was unreachable

```
switch# show ztp information
TFTP Server                : 10.0.0.2
Image File                 : TL_10_02_0001.swi
Configuration File         : ztpv6.cfg
ZTP Status                 : Failed - TFTP server unreachable
HPE ANW Central Location  : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token : NA
Force-Provision           : Enabled
HTTP Proxy Location       : NA
```

Showing a successful switch configuration download from an IPv6 HTTP server

```
switch# show ztp information
HTTP Server                : http://[2001::50]
Image File                 : TL_10_15_0001.swi
Configuration File         : config_file
ZTP Status                 : Success
HPE ANW Central Location  : NA
Alternative HPE ANW Central Location : NA
```

```

HPE ANW Central Shared Token      : NA
Force-Provision                   : Enabled
HTTP Proxy Location                : NA

```

The switch received image and configuration files from a serial-number specific folder on a USB device, and ZTP was successful.

```

switch# show ztp information
TFTP Server                      : NA
Image File                      : usb:/AOSCX/TW88KHD005/GL_10_16_00001.swi
Configuration File              : usb:/AOSCX/TW88KHD005/ztp.cfg
Status                          : Success
HPE ANW Central Location        : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token    : NA
Force-Provision                 : Disabled
HTTP Proxy Location             : NA

```

The switch received image and configuration files from a generic folder on a USB device, and ZTP was successful.

```

switch# show ztp information
TFTP Server                      : NA
Image File                      : usb:/AOSCX/ztp/ML_10_15_1000F.swi
Configuration File              : usb:/AOSCX/ztp/config.cfg
Status                          : Success
HPE ANW Central Location        : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token    : NA
Force-Provision                 : Disabled
HTTP Proxy Location             : NA

```

The switch received an image file from a vendor-class specific folder on a USB device, and ZTP was successful.

```

switch# show ztp information
TFTP Server                      : NA
Image File                      : usb:/AOSCX/8325_JL636A/GL_10_16_1000A.swi
Configuration File              : NA
Status                          : Success
HPE ANW Central Location        : NA
Alternative HPE ANW Central Location : NA
HPE ANW Central Shared Token    : NA
Force-Provision                 : Disabled
HTTP Proxy Location             : NA

```

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
```

Mbr/Slot-Sensor	Module Type	Current 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
```

Mbr/Slot-Sensor	Module Type	Current 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:
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 Disabled, 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.

Switch system and hardware commands

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
8400	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
8400	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
8400	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

Parameter	Description
	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.

fabric admin-state

```
fabric <SLOT-ID> admin-state
    diagnostic
    down
    up
```

Description

Sets the administrative state of the specified fabric module.

Parameter	Description
<SLOT-ID>	Specifies the member and slot of the module. For example, to specify the module in member 1, slot 2, enter the following:

Parameter	Description
	1/2
diagnostic	Selects the diagnostic administrative state. Network traffic does not pass through the module.
down	Selects the down administrative state. Network traffic does not pass through the module.
up	Selects the up administrative state. The module is fully operational. The up state is the default administrative state.

Usage

This command is valid for fabric modules only.

Examples

Setting the administrative state of the fabric module 2 to **down**:

```
switch(config)# fabric 1/2 admin-state down
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	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: <code>switch</code>

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.

Parameter	Description
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
8400	Manager (#)	Administrators or local user group members with execution rights for this command.

module admin-state

```
module <SLOT-ID> admin-state {diagnostic | down | up}
no module <SLOT-ID> [admin-state [diagnostic | down | up]]
```

Description

Sets the administrative state of the specified line module.

The **no** form of the command configures administrative state to the default **up**.

Parameter	Description
<SLOT-ID>	Specifies the member and slot of the module. For example, to specify the module in member 1, slot 3, enter the following: 1/3
diagnostic	Selects the diagnostic administrative state. Network traffic does not pass through the module.
down	Selects the down administrative state. Network traffic does not pass through the module.
up	Selects the up administrative state. The line module is fully operational. The up state is the default administrative state.

Example

Setting the administrative state of the module in slot **1/3** to **down**:

```
switch(config)# module 1/3 admin-state down
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config	Administrators or local user group members with execution rights for this command.

module product-number

```
module <SLOT-ID> product-number [<PRODUCT-NUM>]  
no module <SLOT-ID> [product-number [<PRODUCT-NUM>]]
```

Description

Changes the configuration of the switch to indicate that the specified member and slot number contains, or will contain, a line module.

The **no** form of this command removes the line module and its interfaces from the configuration. If there is a line module installed in the slot, the line module is powered off and then powered on.

Parameter	Description
<SLOT-ID>	Specifies the member and slot in the form m/s , where m is the member number, and s is the slot number.
<PRODUCT-NUM>	Specifies the product number of the line module. For example: JL363A If there is a line module installed in the slot when you execute this command, <PRODUCT-NUM> is optional. The switch reads the product number information from the module that is installed in the slot. If there is no line module installed in the slot when you execute this command, <PRODUCT-NUM> is required.

Usage

The default configuration associated with a line module slot is:

- There is no module product number or interface configuration information associated with the slot. The slot is available for the installation with any supported line module.
- The Admin State is Up (which is the default value for Admin State).

To add a line module to the configuration, you must use the **module** command either before or after you install the physical module.

If you execute the **module** command after you install a line module in an empty slot, you can omit the **<PRODUCT-NUM>** variable. The switch reads the product information from the installed module.

If the module is not installed in the slot when you execute the module command, you must specify a value for the **<PRODUCT-NUM>** variable:

- The switch validates the product number of the module against the slot number you specify to ensure that the right type of module is configured for the specified slot.

For example, the switch returns an error if you specify the product number of a line module for a slot reserved for management modules.

- You can configure the line module interfaces before the line module is installed.

When you install the physical line module in a preconfigured slot, the following actions occur:

- If a product number was specified in the command and it matches the product number of the installed module, the switch initializes the module.
- If a product number was specified in the command and the product number of the module does not match what was specified, the module device initialization fails.

The **no** form of the command removes the line module and its interfaces from the configuration and restores the line module slot to the default configuration.

If there is a line module installed in the slot when you execute the **no** form of the command, the command also powers off and then powers on the module. Traffic passing through the line module is stopped. Management sessions connected through the line module are also affected.

If the slot associated with the line module is in the default configuration, you can remove the module from the chassis without disrupting the operation of the switch.

Examples

Configuring slot 1/1 for future installation of a line module:

```
switch(config)# module 1/1 product-number jl363a
```

Configuring a line module that is already installed in slot 1/1:

```
switch(config)# module 1/1 product-number
```

Attempting to configure slot 1/1 for the future installation of a line module without specifying the product number (returned error shown):

```
switch(config)# module 1/1 product-number
Line module '1/4' is not physically available. Please provide the product
number to preconfigure the line module.
```

Configuring a JL363A line module in a slot that has already been used to configure a different module:

```
switch(config)# no module 1/4
switch(config)# module 1/4 product-number jl363a
```

Removing a module from the configuration:

```
switch(config)# no module 1/1
This command will power cycle the specified line module and restore its default
configuration. Any traffic passing through the line module will be interrupted.
Management sessions connected through the line module will be affected. It
might take a few minutes to complete this operation.

Do you want to continue (y/n)? y
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config	Administrators or local user group members with execution rights for this command.

mtrace

```
mtrace <IPV4-SRC-ADDR> <IPV4-GROUP-ADDR> [lhr <IPV4-LHR-ADDR>] [ttl <HOPS>]
[vrf <VRF-NAME>]
```

Description

Traces the specified IPv4 source and group addresses.

Parameter	Description
<i>IPV4-SRC-ADDR</i>	Specifies the source IPv4 address to trace.
<i>IPV4-GROUP-ADDR</i>	Specifies the group IPv4 address to trace.
<i>lhr <IPV4-LHR-ADDR></i>	Specifies the last hop router address from which to start the trace.
<i>ttl <HOPS></i>	Specifies the Time-To-Live duration in hops. Range: 1 to 255 hops. Default: 8 hops.
<i>vrfr <VRF-NAME></i>	Specifies the name of the VRF. If a name is not specified the default VRF will be used.

Examples

Tracing with source, group, and LHR addresses and TTL:

```
(switch)# mtrace 20.0.0.1 239.1.1.1 lhr 10.1.1.1 ttl 10

Type escape sequence to abort.
```

```
Mtrace from 10.0.0.1 for Source 20.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying full 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 full 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
8400	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
8400	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
8400	Operator (>) or Manager (#)	Operators 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.

For switches that support line modules (such as 8400 switch series) including the **all** parameter displays information for the active management module and all available line modules.



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. For switches that support line modules, including this parameter displays information for and all available line modules.
vsf member <1-10>	Optional. Display boot history for the specified VSF member

Usage

This command displays the boot-index, boot-ID, and up time in seconds for the current boot. If there is a previous boot, it displays boot-index, boot-ID, reboot time (based on the time zone configured in the system) and reboot reasons. Previous boot information is displayed in reverse chronological order.

The output of this command includes the following information:

Parameter	Description
Index	The position of the boot in the history file. Range: 0 to 3.
Boot ID	A unique ID for the boot . A system-generated 128-bit string.
Current Boot, up for <time>	For the current boot, the show boot-history command shows the number of seconds the module has been running on the current software.
<Timestamp>: boot reason	For previous boot operations, the show boot-history command shows the time at which the operation occurred and the reason for the boot. The reason for the boot is one of the following values: ▪ <DAEMON-NAME> crash: The daemon identified by <DAEMON-NAME> caused the module to boot. ▪ Kernel crash: The operating system software associated with the module caused the module to boot. ▪ Uncontrolled reboot: The reason for the reboot is not known. ▪ Reboot requested through database: The reboot occurred because of a request made through the CLI or other API.

Examples

Showing the boot history of the active management module:

```
switch# show boot-history
Management module
=====

Index : 2
Boot ID : c34a2c2499004a02bbeeff4992e1fdbd
Current Boot, up for 1 days 13 hrs 13 mins 27 secs
```

```

Index : 1
Boot ID : bfba9bc486304e57904ac717a0ccbdcd
02 Sep 23 02:55:33 : CPU request reset with 0x20201, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:55:33 : Switch boot count is 2

Index : 0
Boot ID : a88a71b7ca9a4574af7e3b811ddfdc7e
02 Sep 23 02:49:26 : Reboot requested by user, Version: FL.10.14.0000-1619-
ga9ec1805bd442~dirty
02 Sep 23 02:50:02 : Switch boot count is 1

Index : 3
Boot ID : f00ba10c8c44457f83fee303d014a89a
25 Aug 23 10:27:42 : Power on reset with 0x1, Version: FL.10.14.0000-1465-
g9df95249d06b0~dirty
25 Aug 23 10:28:18 : Switch boot count is 3
25 Aug 23 10:29:02 : Primary overtemperature fault detected with 0x2 in PSU 1/1

```

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 | <SLOT-ID>]

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.
<SLOT-ID>	Shows the core dumps for the management module or line module in <SLOT-ID>. <SLOT-ID> specifies a physical location on the switch. Use the format member/slot/port (for example, 1/3/1) for line

Parameter	Description
	modules. Use the format member/slot for management modules. You must specify the slot ID for either the active management module, or the line module.

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

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

Usage

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 systems with fan trays for HPE Aruba Networking 8400 Switch series:

```
switch# show environment fan
```

Fan tray information

Mbr/Tray	Description	Status	Serial Number	Fans
1/1	JL369A 8400 Fan tray	ready	SGXXXXXXXXXX	6
1/2	JL369A 8400 Fan tray	ready	SGXXXXXXXXXX	6
1/3	N/A	empty	N/A	0

Fan information

Mbr/Tray/Fan	Serial Number	Speed	Direction	Status	RPM
1/1/1	SGXXXXXXXXXX	slow	front-to-back	ok	6000
1/1/2	SGXXXXXXXXXX	normal	front-to-back	ok	8000
1/1/3	SGXXXXXXXXXX	medium	front-to-back	ok	11000
1/1/4	SGXXXXXXXXXX	fast	front-to-back	ok	14000
1/1/5	SGXXXXXXXXXX	max	front-to-back	fault	16500
1/1/6	N/A	N/A	N/A	empty	0
1/2/1	SGXXXXXXXXXX	slow	front-to-back	ok	6000
...					

Fan tray information

Mbr/Tray	Description	Status	Serial Number	Fans
1/1	JL369A 8400 Fan tray	ready	SGXXXXXXXXXX	6
1/2	JL369A 8400 Fan tray	ready	SGXXXXXXXXXX	6
1/3	N/A	empty	N/A	0

Fan information

Mbr/Tray/Fan	Serial Number	Speed	Direction	Status	RPM
1/1/1	SGXXXXXXXXXX	slow	front-to-back	ok	6000
1/1/2	SGXXXXXXXXXX	normal	front-to-back	ok	8000
1/1/3	SGXXXXXXXXXX	medium	front-to-back	ok	11000
1/1/4	SGXXXXXXXXXX	fast	front-to-back	ok	14000
1/1/5	SGXXXXXXXXXX	max	front-to-back	fault	16500
1/1/6	N/A	N/A	N/A	empty	0
1/2/1	SGXXXXXXXXXX	slow	front-to-back	ok	6000
...					

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
<i>[detail]</i>	Displays detailed power consumption information.
<i><MEMBER-ID></i>	For VSF supported platforms only. Displays the power consumption information for the specified VSF member. Range: 1-10.

Usage

Power consumed values are updated every 5 seconds. The total power consumed is the total power used in a chassis. The power consumed average is calculated from the total power consumed as a running average over a period of time. The average period has a default of 10 minutes. The period can be configured using **power-consumption-average-period**.

On chassis where power input is not supported, power consumed is displayed as Power Usage and PSU Output Power is displayed as N/A.

The following information is provided for a summary of power consumption:

- line module: power used by line module
- management module: power used by management module

- fabric module: power used by fabric module
- chassis module: power used by chassis module
- fan module: power used by fan module
- power total: total power consumption
- average power: average for total power consumption that is calculated over a given period
- average period: time to calculate power average

For more information, see the video [AOS-CX 10.14 Release Update: Sustainability Update](#).

Example

Showing the power consumption for a 1RU switch:

```
switch# show environment power-consumption
```

Power Consumption Averaging Period : 600 seconds

Name	Description	Power Usage (W)		PSU Output (W)	
		Instant	Average	Instant	Average
1	8360-32Y4C v2 Switch	120.00	111.16	111.00	102.62

Showing the power consumption for a VSF stack:

```
switch# show environment power-consumption
```

Power Consumption Averaging Period : 600 seconds

Name	Description	Power Usage (W)		PSU Output (W)	
		Instant	Average	Instant	Average
1	6200M 24G 4SFP+ Sw	350.00	349.62	300.00	311.50
2	6200M 24G 4SFP+ Sw	300.00	299.50	280.00	275.50

Showing the power consumption for a switch where input reading is not supported:

```
switch# show environment power-consumption
```

Power Consumption Averaging Period : 600 seconds

Name	Description	Power Usage (W)		PSU Output (W)	
		Instant	Average	Instant	Average
1	6200M 24G 4SFP+ Sw	321.00	330.30	N/A	N/A

Showing the power consumption for a switch with multiple line cards, in brief:

```
switch# show environment power-consumption
```

Power Consumption Averaging Period : 600 seconds

Name	Description	Power Usage (W)		PSU Output (W)	
		Instant	Average	Instant	Average
1	6410 v2 Chassis	900.00	905.62	798.00	803.23

Showing the power consumption for a switch with multiple line cards, in detail:

```
switch# show environment power-consumption detail
Power Consumption Averaging Period : 600 seconds
```

Name	Module	Type	Power Usage (W)		PSU Output (W)	
			Instant	Average	Instant	Average
1	chassis	total	1495.00	1499.99	1307.00	1300.67
1/3	line		97.00			
1/4	line		95.00			
1/5	line		90.00			
1/6	line		58.00			
1/7	line		90.00			
1/8	line		93.00			
1/9	line		96.00			
1/10	line		92.00			
1/11	line		100.00			
1/12	line		99.00			
1/1	management		14.00			
1/2	management		13.00			
	other		370.00			

Showing the power consumption for 4 member stack, in detail:

```
switch# show environment power-consumption detail
Power Consumption Averaging Period : 600 seconds
```

Name	Module	Type	Power Usage (W)		PSU Output (W)	
			Instant	Average	Instant	Average
1	chassis	total	930.00	905.17	830.00	803.40
2	chassis	total	900.00	920.00	875.00	880.25
3	chassis	total	850.00	857.25	802.00	805.00
4	chassis	total	1200.00	1100.56	921.00	950.00
Total Power Consumption			3428.00			

Showing the power consumption for VSF member 2:

```
switch# show environment power-consumption member 2
Power Consumption Averaging Period : 600 seconds
```

Name	Description	Power Usage (W)		PSU Output (W)	
		Instant	Average	Instant	Average
2	6200M 24G 4SFP+ Sw	300.00	299.50	280.00	275.50

Showing the power consumption for VSF invalid member:

```
switch# show environment power-consumption member 5
Member 5 is not present
```

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-consumption

`show environment power-consumption [vsx-peer]`

Description

Shows the power being consumed by each management module, line card, and fabric card subsystem, and shows power consumption for the entire chassis.

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

Usage

This command is only applicable to systems that support power consumption readings.

The power consumption values are updated once every minute.

The output of this command includes the following information:

Parameter	Description
Name	Shows the member number and slot number of the management module, line module, or fabric card module.
Type	Shows the type of module installed at the location specified by Name.
Description	Shows the product name and brief description of the module.
Usage	Shows the instantaneous power consumption of the module. Power consumption is shown in Watts.
Module Total Power Usage	Shows the total power consumption of all the modules listed. Power consumption is shown in Watts.
Chassis Total Power Usage	Shows the total instantaneous power consumed by the entire chassis, including modules and components that do not support

Parameter	Description
	individual power reporting. Power consumption is shown in Watts.
Chassis Total Power Available	Shows the total amount of power, in Watts, that can be supplied to the chassis.
Chassis Total Power Allocated	Shows total power, in Watts, that is allocated to powering the chassis and its installed modules.
Chassis Total Power Unallocated	Shows the total amount of power, in Watts, that has not been allocated to powering the chassis or its installed modules. This power can be used for additional hardware you install in the chassis.

For more information, see the video [AOS-CX 10.14 Release Update: Sustainability Update](#).

Example

Showing power consumption usage for an HPE Aruba Networking 8400 switch

```
switch> show environment power-consumption
```

Name	Type	Description	Usage
1/5	management-module	JL368A 8400X Mgmt Mod	97 W
1/6	management-module	JL368A 8400X Mgmt Mod	49 W
1/1	line-card-module	JL363A 8400X 32P 10G SFP/SFP+ Msec Mod	139 W
1/2	line-card-module	JL365A 8400X 8P 40G QSFP+ Adv Mod	158 W
1/3	line-card-module	JL366A 8400X 6P 40G/100G QSFP28 Adv Mod	127 W
1/4	line-card-module	JL363A 8400X 32P 10G SFP/SFP+ Msec Adv Mod	148 W
1/7	line-card-module	JL363A 8400X 32P 10G SFP/SFP+ Msec Adv Mod	152 W
1/8	line-card-module	JL363A 8400X 32P 10G SFP/SFP+ Msec Adv Mod	125 W
1/9	line-card-module	JL363A 8400X 32P 10G SFP/SFP+ Msec Adv Mod	132 W
1/10	line-card-module	JL363A 8400X 32P 10G SFP/SFP+ Msec Adv Mod	143 W
1/1	fabric-card-module	JL367A 8400X 7.2Tbps Fab Mod	107 W
1/2	fabric-card-module	JL367A 8400X 7.2Tbps Fab Mod	93 W
1/3	fabric-card-module	JL367A 8400X 7.2Tbps Fab Mod	87 W
Module Total Power Usage			1557 W
Chassis Total Power Usage			1807 W
Chassis Total Power Available			9990 W
Chassis Total Power Allocated (total of all max wattages)			4130 W
Chassis Total Power Unallocated			5860 W

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show environment power-supply

```
show environment power-supply
  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.
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:

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 rear-display-module

show environment rear-display-module [vsx-peer]

Description

Shows information about the display module on the back of the switch.

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

Example

Showing the rear display module information on the back of the switch:

```
switch> show environment rear-display-module

Rear display module is ready
Description: 8400 Rear Display Mod
Full Description: 8400 Rear Display Module
Serial number: SG00000000
Part number: 5300_0272
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Operator (>) or Manager (#)	Operators 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

Showing current temperature information for an 8400 switch:

```
switch# show environment temperature
```

```
Temperature information
```

```
-----
Mbr/Slot-Sensor      Module Type      Current
temperature          Status
-----
1/1-PCIE-Switch      line-card-module 95.82 C         normal
```

1/1-Processor	line-card-module	0.00 C	fault
1/1-Switch-ASIC	line-card-module	116.36 C	emergency
1/1-Switch-ASIC-Internal	line-card-module	108.25 C	critical
1/2-PCIE-Switch	line-card-module	95.82 C	normal
...			

Showing detailed temperature information for an 8400 switch:

```
switch# show environment temperature detail

Detailed temperature information
-----
Mbr/Slot-Sensor      : 1/1-PCIE-Switch
Module Type          : line-card-module
Module Description    : JL363A 8400X 32P 10G SFP/SFP+ Msec Mod
Status                : normal
Fan-state            : normal
Current temperature   : 95.82 C
Minimum temperature   : 93.52 C
Maximum temperature   : 96.15 C
...

Detailed temperature information
-----
Mbr/Slot-Sensor      : 1/1-PCIE-Switch
Module Type          : line-card-module
Module Description    : JL363A 8400X 32P 10G SFP/SFP+ Msec Mod
Status                : normal
Fan-state            : normal
Current temperature   : 95.82 C
Minimum temperature   : 93.52 C
Maximum temperature   : 96.15 C
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show events

```
show events [ -e <EVENT-ID> |
-s {emergency | alert | critical | error | warning | notice | info | debug} |
-r |
-a |
-n <COUNT> |
-i <MEMBER-SLOT> |
```

```
-m {active | standby} |
-c {lldp | ospf | ...} |
-d {lldpd | bgpd | fand | ...}]
```

Description

Shows event logs generated by the switch modules since the last reboot.

Parameter	Description
<code>-e <EVENT-ID></code>	Shows the event logs for the specified event ID. Event ID range: 101 through 99999.
<code>-s {emergency alert critical error warning notice info debug}</code>	Shows the event logs for the specified severity. Select the severity from the following list: ▪ 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.
<code>-r</code>	Shows the most recent event logs first.
<code>-a</code>	Shows all event logs, including those events from previous boots.
<code>-n <COUNT></code>	Displays the specified number of event logs.
<code>-i <MEMBER-SLOT></code>	Shows the event logs for the specified slot ID.
<code>-m {active standby}</code>	Shows the event logs for the specified management card role. Selecting active displays the event log for the AMM management card role and standby displays event logs for the SMM management card role.
<code>-c {lldp ospf ...}</code>	Shows the event logs for the specified event category. Enter show event -c for a full listing of supported categories with descriptions.
<code>-d {lldpd bgpd fand ...}</code>	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 management card role:

```
switch# show events -m active
-----
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 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 fabric

```
show fabric [<SLOT-ID>] [vsx-peer]
```

Description

Shows information about the installed fabrics.

Parameter	Description
<code><SLOT-ID></code>	Specifies the member and slot of the fabric to show. For example, to show the module in member 1, slot 2, enter the following: 1/2
<code>vsx-peer</code>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing all fabrics:

```
switch# show fabric

Fabric Modules
=====

      Product
Slot Number Description                Serial Number  Status
-----
1/1  JL367A  8400X 7.2Tbps Fab Mod             SG00000000  Ready
1/2  JL367A  8400X 7.2Tbps Fab Mod             SG00000000  Initializing
1/3  JL367A  8400X 7.2Tbps Fab Mod             SG00000000  Initializing
```

Showing a single fabric:

```
switch# show fabric 1/1

Fabric module 1/1 is ready
Admin state: Up
Description: 8400X 7.2Tbps Fab Mod
Full Description: HPE_ANW 8400X 7.2Tbps Fabric Module
Serial number: SG00000000
Product number: JL367A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) 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:

```
switch# show images

-----
AOS-CX Primary Image
-----
Version : XL.xx.xx.xxxx
Size    : 141 MB
Date    : 2017-06-30 14:02:34 PDT
SHA-256 : 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

-----
AOS-CX Secondary Image
-----
Version : XL.xx.xx.xxxx
Size    : 143 MB
Date    : 2017-06-30 14:02:34 PDT
SHA-256 : 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

Default Image : secondary

-----
Management Module 1/5 (Active)
-----
Active Image      : primary
Service OS Version : GT.01.01.0001
BIOS Version      : GT-01-0013

-----
Management Module 1/6 (Standby)
-----
Active Image      : secondary
Service OS Version : GT.01.01.0001
BIOS Version      : GT-01-0013
```

```
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 hardware and software IP error statistics for packets received by the switch since the switch was last booted. If none of the optional VRF parameters are included, the **show ip errors** command displays the current system-wide hardware IP error counters and the default VRF's software IP error counters on the switch.

Parameter	Description
vrf <vrf-name>	Optional. Display hardware and software IP error counters for a specific VRF.
all-vrfs	Optional. Display hardware and software IP error counters for all VRFs

Usage

IP error info about received packets is collected from each active line card on the switch and is preserved during failover events. Error counts are cleared when the switch is rebooted.

Drop reasons may include the following:

■ Malformed packet

The packet does not conform to TCP/IP protocol standards such as packet length or internet header length.

A large number of malformed packets can indicate that there are hardware malfunctions such as loose cables, network card malfunctions, or that a DOS (denial of service) attack is occurring.

■ IP address error

The packet has an error in the destination or source IP address. Examples of IP address errors include the following:

- The source IP address and destination IP address are the same.
- There is no destination IP address.
- The source IP address is a multicast IP address.
- The forwarding header of an IPv6 address is empty.
- There is no source IP address for an IPv6 packet.

■ Invalid TTLS

The TTL (time to live) value of the packet reached zero. The packet was discarded because it traversed the maximum number of hops permitted by the TTL value.

TTLs are used to prevent packets from being circulated on the network endlessly.

Example

Showing the current system-wide hardware IP error counters and the default VRF's software IP error counters on the switch:

```
switch# show ip errors
System-wide (hardware) IP errors
-----
Drop reason                               Packets
-----
Malformed packets                         1
IP address errors                         10
Per-VRF (software) IP errors
-----
VRF
Drop reason                               Packets
-----
default
IPv4 maximum transmission unit             3
IPv4 time to live                          0
IPv6 maximum transmission unit             0
IPv6 hop limit                            6
-----
Malformed packets                          1
...

```

Showing the current system-wide hardware IP error counter and the software IP error counter for all VRFs on the switch.

```
switch# show ip errors all-vrfs
System-wide (hardware) IP errors
-----
Drop reason                               Packets
-----
Malformed packets                         1
IP address errors                         10
Per-VRF (software) IP errors
-----
VRF
Drop reason                               Packets
-----
default
IPv4 maximum transmission unit             3
IPv4 time to live                          0

```

```

IPv6 maximum transmission unit      0
IPv6 hop limit                      6
red
IPv4 maximum transmission unit      3
IPv4 time to live                   7
IPv6 maximum transmission unit      0
IPv6 hop limit                      6
blue
IPv4 maximum transmission unit      0
IPv4 time to live                   1
IPv6 maximum transmission unit      0
IPv6 hop limit                      6
...

```

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
8400	Operator (>) or Manager (#)	Operators 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 [<SLOT-ID>] [vsx-peer]

Description

Shows information about installed line modules and management modules.

Parameter	Description
<SLOT-ID>	Specifies the member and slot numbers in format member/slot. For example, to show the module in member 1, slot 3, enter 1/3.
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.

If you use the `<slot-id>` parameter to specify a slot that does not have a line module installed, a message similar to the following example is displayed:

```
Module 1/4 is not physically present.
```

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 module is the active management module.

Standby

This module is the standby management module.

Deinitializing

The module is being deinitialized.

Diagnostic

The module is in a state used for troubleshooting.

Down

The module is physically present but is powered down.

Empty

The module hardware is not installed in the chassis.

Failed

The module has experienced an error and failed.

Failover

This module 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 module is being initialized.

Present

The module hardware is installed in the chassis.

Ready

The module is available for use.

Updating

A firmware update is being applied to the module.

Examples

Showing all installed modules on an 8400 switch:

```
switch# show module
```

```
Management Modules
```

```
=====
```

	Product		Serial	
Slot	Number	Description	Number	Status
1/5	JL368A	8400 Mgmt Mod	SG00000000	Active
1/6	JL368A	8400 Mgmt Mod	SG00000000	Standby

```
Line Modules
```

```
=====
```

	Product		Serial	
Slot	Number	Description	Number	Status
1/1	JL363A	8400X 32P 10G SFP/SFP+ Msec Mod	SG00000000	Down
1/3	JL365A	8400X 8P 40G QSFP+ Adv Mod	SG00000000	Ready
1/4	JL366A	8400X 6P 40G/100G QSFP28 Adv Mod	SG00000000	Initializing
1/8	JL365A	8400X 8P 40G QSFP+ Adv Mod	SG00000000	Ready


```
1/10 JL365A 8400X 8P 40G QSFP+ Adv Mod      SG00000000 Ready
...
```



The output of this show command may seem to indicate that a JL363A Line card supports MACsec. This line card is hardware-ready to support MACsec, but this feature is not currently support for this line card in AOS-CX software.

Showing a management module on an 8400 switch:

```
switch# show module 1/5

Management module 1/5 is active
Admin state: Up
Description: 8400 Mgmt Mod
Full Description: 8400 Management Module
Serial number: SG00000000
Product number: JL368A
```

Showing a slot that does not contain a line module:

```
switch(config)# show module 1/3
Module 1/3 is not physically present
```

Showing a line module after removing it from the configuration with **no module** command, but the hardware remains installed in the slot:

```
switch(config)# show module 1/1

Line module 1/1 is ready
Admin state: Up
Description: 8400X 32P 10G SFP/SFP+ Msec Mod
Full Description: 8400X 32-port 10GbE SFP/SFP+ with MACsec Advanced Module
Serial number: SG00000000
Product number: JL363A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show running-config

```
show running-config [<FEATURE>] [all] [vsx-peer]
```

Description

Shows the current nondefault configuration running on the switch. No user information is displayed.

Parameter	Description
<FEATURE>	Specifies the name of a feature. For a list of feature names, enter the <code>show running-config</code> command, followed by a space, followed by a question mark (?). When the <code>json</code> parameter is used, the <code>vsx-peer</code> parameter is not applicable.
<i>all</i>	Shows all default values for the current running configuration.
<i>vsx-peer</i>	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version AOS-CX 10.0X.XXXX
!
lldp enable
linecard-module LC1 part-number JL363A
vrf green
!
!
!
!
!
!
aaa authentication login default local
aaa authorization commands default none
!
!
!
!
vlan 1
    no shutdown
vlan 20
    no shutdown
vlan 30
    no shutdown
interface 1/1/1
    no shutdown
    no routing
    vlan access 30
interface 1/1/32
    no shutdown
    no routing
    vlan access 20
interface bridge_normal-1
    no shutdown
```

```

interface bridge_normal-2
  no shutdown
interface vlan20
  no shutdown
  vrf attach green
  ip address 20.0.0.44/24
  ip ospf 1 area 0.0.0.0
  ip pim-sparse enable

interface vlan30
  no shutdown
  vrf attach green
  ip address 30.0.0.44/24
  ip ospf 1 area 0.0.0.0
  ip pim-sparse enable

  ip pim-sparse hello-interval 100

```

Showing the current running configuration in json format:

```

switch> show running-config json
Running-configuration in JSON:
{
  "Monitoring_Policy_Script": {
    "system_resource_monitor_mm1.1.0": {
      "Monitoring_Policy_Instance": {
        "system_resource_monitor_mm1.1.0/system_resource_monitor_
mm1.1.0.default": {
          "name": "system_resource_monitor_mm1.1.0.default",
          "origin": "system",
          "parameters_values": {
            "long_term_high_threshold": "70",
            "long_term_normal_threshold": "60",
            "long_term_time_period": "480",
            "medium_term_high_threshold": "80",
            "medium_term_normal_threshold": "60",
            "medium_term_time_period": "120",
            "short_term_high_threshold": "90",
            "short_term_normal_threshold": "80",
            "short_term_time_period": "5"
          }
        }
      }
    },
    ...
    ...
    ...
    ...

```

Show the current running configuration without default values:

```

switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!

```

```

!
!
!
!
!
vlan 1
switch(config)# show running-config all
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
!
!
!
!
!
vlan 1
switch(config)#

```

Show the current running configuration with default values:

```

switch(config)# snmp-server vrf mgmt
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
snmp-server vrf mgmt
!
!
!
!
!
vlan 1
switch(config)#
switch(config)#
switch(config)# show running-config all
Current configuration:
!
!Version AOS-CX Virtual.10.04.0000-6523-gbb15c03~dirty
led locator on
!
!
!
!
!
snmp-server vrf mgmt
snmp-server agent-port 161
snmp-server community public
!
!
!
!
!

```

```
vlan 1
switch(config)#
```

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	<code>config</code> or a child of <code>config</code> . See Usage.	Administrators or local user group members with execution rights for this command.

show startup-config

`show startup-config [json]`

Description

Shows the contents of the startup configuration.



Switches in the `factory-default` configuration do not have a startup configuration to display.

Parameter	Description
<code>json</code>	Display output in JSON format.

Examples

Showing the startup-configuration in non-JSON format:

```
switch# show startup-config
Startup configuration:
!
!Version AOS-CX XL.xx.xx.xxxx
!export-password: default
hostname BLDG03-F1
user admin group administrators password ciphertext AQBapfYzQNiCPJ/
JNSu7YNfaCzlWEnWFlwLfkARd8OG6yPpcYgAAABXRe9joTRtF1S1b4b09teMfMN3POKdQk+

br6SjSXGG40BB3ilZ8ym9qqSRkr84FEdq6w5uR2IGciVC5tBnZMrWCim0KR20XcQ5rFj/TMBvTkhQ8bJpS
YG8nMh
module 1/3 product-number j1365a
module 1/1 product-number j1363a
module 1/2 product-number j1363a
cli-session
    timeout 0
!
!
!
ssh server vrf mgmt
ssh certified-algorithms-only
!
!
!
!
!
vlan 1,195,197-200,4000
interface mgmt
    no shutdown
    ip static 10.6.9.24/24
    default-gateway 10.6.9.1
interface 1/1/1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1,197-200
interface vlan200
    ip address 10.3.200.3/24
ip route 0.0.0.0/0 10.3.200.1
https-server rest access-mode read-write
https-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 error-counter-monitor

`show system error-counter-monitor {basic <PORT-NUM> | extended} [vsx-peer]`

Description

Shows error counter statistics.

Parameter	Description
<code>basic <PORT-NUM></code>	Specifies a physical port on the switch. Use the format member/slot/port (for example, 1/3/1).
<code>extended</code>	Shows statistics for all interfaces.

Examples

Showing error counter statistics for interface 1/1/1:

```
switch# show system error-counter-monitor basic 1/1/1

Interface error counter statistics for 1/1/1

Error Counter                               Value
-----
EtherStatsOversizePkts                      983
EtherStatsUndersizePkts                    1024
EtherStatsJabbers                           10
Dot3StatsAlignmentErrors                   462
Dot3StatsFCSErrors                         321
Dot3StatsLateCollisions                    2024
EtherStatsFragments                        121
Dot3StatsExcessiveCollisions               1025
IfInBroadcastPkts                          2001
```

Showing error counter statistics for all interfaces:


```
switch# show system error-counter-monitor extended
```

```
Interface error counter statistics for 1/1/1
```

Error Counter	Value
EtherStatsOversizePkts	983
EtherStatsUndersizePkts	1024
EtherStatsJabbers	10
Dot3StatsAlignmentErrors	462
Dot3StatsFCSErrors	321
Dot3StatsLateCollisions	2024
EtherStatsFragments	121
Dot3StatsExcessiveCollisions	1025
IfInBroadcastPkts	2001
...	
...	

```
Interface error counter statistics for 1/8/32
```

Error Counter	Value
EtherStatsOversizePkts	0
...	

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	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  : XXXXXXXXXXXX
Base MAC Address    : xxxxxx-xxxxxx
AOS-CX Version      : XX.99.99.9999

Time Zone           : UTC

Up Time             : 1 week, 5 hours, 28 minutes
CPU Util (%)         : 5
CPU Util (% avg 1 min) : 11
CPU Util (% avg 5 min) : 10
Memory Usage (%)     : 35
```

Showing the Service OS password prompt status:

```
switch# show system serviceos password-prompt
password-prompt: disabled
```

Showing system information for a VSX primary and secondary (peer) switch:

```
switch# show system
Hostname           : vsx-primary
System Description  : switch description
System Contact      : contact
System Location     : location

Vendor             : Aruba
Product Name        : XXXXXX ...
Chassis Serial Nbr  : XXXXXXXXXXXX
Base MAC Address    : xxxxxx-xxxxxx

Hostname           : vsx-primary
System Description  : switch description
System Contact      : contact
System Location     : location

Vendor             : Aruba
Product Name        : XXXXXX ...
Chassis Serial Nbr  : XXXXXXXXXXXX
Base MAC Address    : xxxxxx-xxxxxx
AOS-CX Version      : XX.99.99.9999
```

```

Time Zone                : UTC

Up Time                  : 1 week, 2 hours, 15 minutes
CPU Util (%)             : 15
CPU Util (% avg 1 min)   : 12
CPU Util (% avg 5 min)   : 8
Memory Usage (%)         : 37

```

```

switch# show system vsx-peer
Hostname                  : vsx-secondary
System Description       : switch description
System Contact           : contact
System Location          : location

Vendor                   : Aruba
Product Name             : XXXXXX ...
Chassis Serial Nbr       : XXXXXXXXXXXX
Base MAC Address         : xxxxxx-xxxxxx
AOS-CX Version           : XX.99.99.9999

Time Zone                : UTC

CPU Util (%)             : 7
CPU Util (% avg 1 min)   : 13
CPU Util (% avg 5 min)   : 9
Memory Usage (%)         : 32

```

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>] |
    standby | module <SLOT-ID>] [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>.
standby	Shows only the resource utilization data for the standby management module.
module <SLOT-ID>	Shows only the resource utilization data for the line module identified by <SLOT-ID>.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

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-mgmd               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 resource utilization data for the standby management module:

```
switch# show system resource-utilization standby
System Resources:
Processes                : 244
CPU usage(%)             : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%)          : 11
Open FD's                : 1854
Storage 1: Endurance utilization = 18% (ssd), Health = normal

Data written to various partitions since boot
Nos      : 15 MB
Log      : 1 MB
Coredump : 23 MB
Security : 2 MB
Selftest : 405 KB
Swap     : 14 MB

Storage partition usage(%)
Nos      : 5
Log      : 60
Coredump : 23
Security : 2
Selftest : 1
Swap     : 0

Process                CPU Usage(%)    Memory Usage(%)  Open FD's
-----
hpe-sysmond            1                2                11
hpe-mgmdd              0                1                5
...
```

Showing resource utilization data for a line module:

```
switch# show system resource-utilization module 1/1
-----
System Resource utilization for line card module: 1/1
-----
```

```

CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 754

Data written to various partitions since boot
Coredump : 23 MB

Storage partition usage(%)
Coredump : 45

```

Showing resource utilization data for all modules:

```

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 = 17% (ssd), 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

aaa

utilspamcfg      0             1                10

-----
Resource utilization data for Standby 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 = 17% (ssd), 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

```

System Resource utilization for line card module: 1/7

```

CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 480

```

Data written to various partitions since boot

```

Coredump : 23 MB

```

Storage partition usage(%)

```

Coredump : 23

```

System Resource utilization for line card module: 1/8

```

CPU usage(%) : 10
CPU usage(% average over 1 minute) : 11
CPU usage(% average over 5 minute) : 15
Memory usage(%) : 11
Open FD's : 485

```

Data written to various partitions since boot

```

Coredump : 23 MB

```

Storage partition usage(%)

```

Coredump : 47

```

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
<code>basic</code>	Specifies showing a basic set of information.
<code><FEATURE></code>	Specifies the name of a feature. For a list of feature names, enter the <code>show tech</code> command, followed by a space, followed by a question mark (?).
<code>local-file</code>	Shows the output of the <code>show tech</code> command to a local text file.

Usage

To terminate the output of the `show tech` command, enter **Ctrl+C**.

If the command was not terminated with **Ctrl+C**, at the end of the output, the `show tech` command shows the following:

- The time consumed to execute the command.
- The list of failed `show` commands, if any.

To get a copy of the local text file content created with the `show tech` command that is used with the `local-file` parameter, use the `copy show-tech local-file` command.

Example

Showing the basic set of system information:

```
switch# show tech basic
=====
Show Tech executed on Wed Sep  6 16:50:37 2017
=====
[Begin] Feature basic
=====

*****
Command : show core-dump all
*****
```



```

no core dumps are present

...
=====
[End] Feature basic
=====

=====
1 show tech command failed
=====
Failed command:
  1. show boot-history
=====
Show tech took 3.000000 seconds for execution

```

Directing the output of the **show tech basic** command to the local text file:

```

switch# show tech basic local-file
Show Tech output stored in local-file. Please use 'copy show-tech local-file'
to copy-out this file.

```

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 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 8400 switch::

```
switch> show version
-----
AOS-CX
(c) Copyright 2022 Hewlett Packard Enterprise Development LP
-----

Version       : XL.xx.xx.xxxx
Build Date    : 2022-05-27 17:00:46 PDT
Build ID      : AOS-CX:XL.xx.xx.xxxx:2b4032a4282b:201707241803
Build SHA     : 2b4032a4282b47ab94ea92a1436e1194f34bb5ba
Active Image  : secondary

Service OS Version : GT.01.01.0010
BIOS Version      : GT-01-0020
```

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 error-counter-monitor

```
system error-counter-monitor
no system error-counter-monitor
```

Description

Enables the system error counter monitoring feature, which records error counter data every 10 seconds. Default: Disabled.

The **no** form of the command disables error counter monitoring and stops the recording of error counter data.

Example

Enabling the system error counter monitor:

```
switch(config)# system error-counter-monitor
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config	Administrators or local user group members with execution rights for this command.

system error-counter-monitor poll-interval

```
system error-counter-monitor poll-interval <INTERVAL>
```

Description

Sets the polling interval used for the collection and recording of error counter data.

Parameter	Description
<INTERVAL>	Specifies the poll interval in seconds. Range: 10 to 3600. Default: 10.

Example

Setting the system error counter monitor poll interval:

```
switch(config)# system error-counter-monitor poll-interval 20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
8400	config	Administrators or local user group members with execution rights for this command.

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.

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.com/notifications/subscriptions> (requires an active HPE Aruba Networking Support Portal account to manage subscriptions). Security notices are viewable without an HPE Aruba Networking Support Portal account.

Warranty Information

To view warranty information for your product, go to <https://www.arubanetworks.com/support-services/product-warranties/>.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at <https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

Additional regulatory information

HPE Aruba Networking is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see <https://www.arubanetworks.com/company/about-us/environmental-citizenship/>.

Documentation Feedback

HPE Aruba Networking is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback

(docsfeedback-switching@hpe.com). 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.