AOS-CX 10.10 Fundamentals Guide

6300, 6400 Switch Series

aruba

a Hewlett Packard
Enterprise company

Contents

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

Applicable products

This document applies to the following products:

- Aruba 6300 Switch Series (JL658A, JL659A, JL660A, JL661A, JL662A, JL663A, JL664A, JL665A, JL666A, JL667A, JL668A, JL762A, R8S89A, R8S90A, R8S91A, R8S92A)
- Aruba 6400 Switch Series (JL762A, R0X31A, R0X38B, R0X39B, R0X40B, R0X41A, R0X42A, R0X43A, R0X44A, R0X45A, R0X26A, R0X27A, JL741A)

Latest version available online

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

Command syntax notation conventions

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

Convention	Usage
`{ }`	Braces. Indicates that at least one of the enclosed items is required.
`[ ]`	Brackets. Indicates that the enclosed item or items are optional.
… or `...`	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

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

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

Understanding the CLI prompts

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

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

   Indicates the operator command context.
`switch#`

   Indicates the manager command context.

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

   Indicates the configuration context for a feature. For example:
`switch(config-if)#`

   Identifies the `interface` context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:
`switch(config-vlan-100)#`

When referring to this context, this document uses the syntax:
`switch(config-vlan-`*<VLAN-ID>*`)#`

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

Identifying switch ports and interfaces

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

On the 6300 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 10. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

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

On the 6400 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 1/1 and 1/2.
  - Line modules are on the front of the switch starting in slot 1/3.
- *port*: Physical number of a port on a line module.

For example, the logical interface `1/3/4` in software is associated with physical port 4 in slot 3 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 Aruba 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 Aruba 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.

Aruba Network Analytics Engine introduction

The Aruba 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 Aruba 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.

Aruba CX mobile app

The Aruba CX 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.

For more information about the Aruba CX mobile app, see:

www.arubanetworks.com/products/networking/switches/cx-mobileapp.

Aruba NetEdit

Aruba 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 Aruba NetEdit, search for NetEdit at the following website:

www.hpe.com/support/hpesc

Ansible modules

Ansible is an open-source IT automation platform.

Aruba 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 Aruba 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`, and `DELETE` methods.

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

In-band and out-of-band management

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

In band

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

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

Out of band

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

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

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

SNMP-based management support

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

User accounts

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

Two types of user accounts are supported:

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

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 Aruba CX 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 Aruba CX 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.

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. If your network administrator or installation site coordinator has instructed you to connect network cable to a data port, connect the cable to that data port instead.

   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 Aruba CX 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 Aruba CX 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 Aruba CX mobile app in the Apple Store or Google Play.
- The Aruba CX 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. On the 6400, the active management module is typically installed in slot 1. When configuring a stack, a USB Bluetooth adapter must be installed on each 6300 switch in the stack.

   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 Aruba CX 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 Aruba CX mobile app, see the online help for the application.

Troubleshooting Bluetooth connections

Bluetooth connection IP addresses

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

Switch
    192.168.99.1
Mobile device
    192.168.99.10

Bluetooth is connected but the switch is not reachable

Symptom

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

Solution 1

Cause

The mobile device is paired with a different nearby switch.

Action

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

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

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

   A switch supports one active Bluetooth connection at a time.

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

Solution 2

Cause

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

Action

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

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

Bluetooth is not connected

Symptom

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

Solution 1

Cause

Bluetooth is not enabled on your mobile device.

Action

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

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

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

A switch supports one active Bluetooth connection at a time.

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

Solution 2

Cause

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

Action

Move closer to the switch.

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

Solution 3

Cause

Your mobile device is not paired with the switch.

Action

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

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

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

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

Solution 4

Cause

Bluetooth is not enabled on the switch.

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

Action

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

- Use the `show bluetooth` CLI command to show the Bluetooth configuration and the status of the Bluetooth adapter.
- To enable the USB port, enter the CLI command: `usb`
- An inserted USB drive must be mounted each time the switch boots or fails over to a different management module. To mount the drive, enter the CLI command: `usb mount`
- To enable Bluetooth, enter the CLI command: `bluetooth enable`

Solution 5

Cause

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

Action

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

   Use the `show bluetooth` CLI command to show the Bluetooth configuration and the status of the Bluetooth adapter.

2. Either disconnect the other device or use that device to communicate with the switch.

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

Solution 6

Cause

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

Action

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

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

   `Switch_model-Serial_number`

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

   A switch supports one active Bluetooth connection at a time.

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

Solution 7

Cause

The USB Bluetooth adapter is not installed in the switch.

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

Action

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

For switches that have multiple management modules, you must install the USB Bluetooth adapter in the USB port of the active management module. Typically, for new switches, the active management module is the module in slot 5 (Aruba 8400 switches) or slot 1 (Aruba 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 Aruba X2 C2 RJ45 to DB9 console cable. (6400 only), or a USB-C cable (6300/6400).

Procedure

1. Connect the console port on the switch to the serial port on the computer using a console cable, or connect the USB-C port on the switch to the USB-C port on the computer using a USB-C 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 login.

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.

Configure using DHCP or static IP

Users can use any data ports for in-band management purposes. IP DHCP is supported on interface VLAN 1 only. All switch ports are part of access VLAN 1 by default. Static IP address and IP DHCP configuration can co-exist on VLAN 1, however static addresses take precedence whenever configured.

DHCP Configuration

```
switch#: config
switch(config)#: vlan 1
Switch(config-vlan-1)#: description Management VLAN
Switch(config-vlan-1)#: end
Switch#
!
Switch(config)#: interface 1/1/1
Switch(config-if)#: description IN-BAND Management Port
Switch(config-if)#: vlan access 1
Switch(config-if)#: no shutdown
Switch(config-if)#: end
Switch#
!
Switch(config)#: interface vlan 1
Switch(config-if-vlan)#: description IN-BAND Management Interface
Switch(config-if-vlan)#: ip dhcp
Switch(config-if-vlan)#: no shutdown
Switch(config-if-vlan)#: end
Switch#
!
```

Without DHCP Configuration

```
switch#: config
switch(config)#: vlan 1
Switch(config-vlan-1)#: description Management VLAN
Switch(config-vlan-1)#: end
Switch#
!
Switch(config)#: interface 1/1/1
Switch(config-if)#: description IN-BAND Management Port
Switch(config-if)#: vlan access 1
Switch(config-if)#: no shutdown
Switch(config-if)#: end
Switch#
!
Switch(config)#: interface vlan 1
Switch(config-if-vlan)#: description IN-BAND Management Interface
Switch(config-if-vlan)#: no ip dhcp
Switch(config-if-vlan)#: ip address 192.168.10.1/24
Switch(config-if-vlan)#: no shutdown
Switch(config-if-vlan)#: end
Switch#
```

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`.
3. By default, NTP traffic is sent on the default VRF. If you want to send NTP traffic on the management VRF, use the command `ntp vrf`.
4. Review your NTP configuration settings with the commands `show ntp servers` and `show ntp status`.
5. See the current switch time, date, and time zone with the command `show clock`.

Example

This example creates the following configuration:

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

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

Configuring banners

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

```
switch(config)# banner motd ^
Enter a new banner. Terminate the banner with the delimiter you have chosen.
>> This is an example of a banner text which a connecting user
>> will see before they are prompted for their password.
>>
>> As you can see it may span multiple lines and the input
>> will be terminated when the delimiter character is
>> encountered.^
Banner updated successfully!
```

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

```
switch(config)# banner exec &
Enter a new banner. Terminate the banner with the delimiter you have chosen.
>> This is an example of a different banner text. This time
>> the banner entered will be displayed after a user has
>> authenticated.
>>
>> & This text will not be included because it comes after the '&'
Banner updated successfully!
```

Configuring in-band management on a data port

Prerequisites

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

Procedure

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

For example:

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

4. Enable the Web UI on the interface (on the default VRF) with the command `https-server vrf default`.

    For example:

    ```
    switch(config)# https-server vrf default
    ```

Using the Web UI

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

The Web UI is enabled by default on the default VRF.

Prerequisites

- A connection to the switch CLI.

Procedure

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

    For example:

    ```
    switch# config
    switch(config)# https-server vrf mgmt
    ```

3. Start your web browser and enter the IP address of the management port in the address bar,

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

Configuring the management interface

Prerequisites

A connection to the console port.

Procedure

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

Examples

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

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

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

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

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

IP prefix priority

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

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

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

See also IP Prefix priority commands.

System profiles and configurable IP prefix priority

(Applicable to the 6400 Switch Series.) System profiles set the overall capabilities and capacities of the switch (including IP prefix partitions), based on the selected profile used at boot time. Only certain profiles support configurable IP prefix priority.

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

See also Selecting the system profile.

IP prefix priority defaults

(Applicable to the 6400 Switch Series.) This default IP prefix priority information only applies to system profiles specifically named here. Any profile unnamed here does not support configurable IP prefix priority. Some profiles require six IP prefix values and others require five IP prefix values.

6300 Switch Series (no profiles), (six prefix values required):

- **IPv4**: 24, 23, 22, 21, 16, 8
- **IPv6**: 64, 48, 46, 44, 40, 36

6400 Switch Series, V1 modules, profile: **default**, v2 modules profiles: **default**, **V2-default** (six prefix values required):

- **IPv4**: 24, 23, 22, 21, 16, 8
- **IPv6**: 64, 48, 46, 44, 40, 36

6400 Switch Series, V2 modules, profile: **v2-Core-High-Bandwidth** (five prefix values required):

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

IP Prefix priority commands

ip prefix-priority

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

Description

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

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

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

Parameter	Description
<PREFIX-LENGTHS>>	Specifies a space-separated list of exactly five or six prefix lengths, in descending order. Range: 8 to 31. On the 6300 Switch Series, six prefix lengths are used. On the 6400 Switch Series, six prefix lengths are used for profiles **default** and **V2-default**, and five prefix lengths are used for profile **v2-Core-High-Bandwidth**.

Examples

Configuring custom IPv4 route prefix lengths:

```
switch(config)# ip prefix-priority 29 28 27 24 23 16
Save this config and reboot the switch for the changes to take effect
...
```

Resetting IPv4 route prefix lengths to their default:

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

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

```
switch(config)# ip prefix-priority 28 29 27 23 24 16
Prefix lengths must be specified in descending order
```

Attempting to configure eight prefix lengths:

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

Attempting to configure three prefix lengths:

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

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6300 6400	config	Administrators or local user group members with execution rights for this command.

ipv6 prefix-priority

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

Description

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

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

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

Parameter	Description
<PREFIX-LENGTHS>>	Specifies a space-separated list of exactly five or six prefix lengths, in descending order. Range: 8 to 64. On the 6300 Switch Series, six prefix lengths are used. On the 6400 Switch Series, six prefix lengths are used for profiles **default** and **V2-default**, and five prefix lengths are used for profile **v2-Core-High-Bandwidth**.

Examples

Configuring custom IPv6 route prefix lengths:

```
switch(config)# ipv6 prefix-priority 64 63 62 32 31 28
Save this config and reboot the switch for the changes to take effect
...
```

Resetting IPv6 route prefix lengths to their default:

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

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

```
switch(config)# ipv6 prefix-priority 64 62 63 31 32 28
Prefix lengths must be specified in descending order
```

Attempting to configure eight prefix lengths:

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

Attempting to configure three prefix lengths:

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

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6300 6400	config	Administrators or local user group members with execution rights for this command.

show ip prefix-priority

```
show ip prefix-priority
```

Description

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

Examples

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

```
switch# show ip prefix-priority

 IP Exact-Prefix Table Information

 Configuration Status: Ready to apply on next reboot

         Default    Current    Pending
 Table    Length    Length     Length
 ---------------------------------
 1          24        24         29*
 2          23        23         28*
 3          22        22         27*
 4          21        21         24*
 5          16        16         23*
 6           8         8         16*

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

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 prefix-priority

```
show ipv6 prefix-priority
```

Description

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

Examples

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

```
switch# show ipv6 prefix-priority

 IPv6 Exact-Prefix Table Information

 Configuration Status: Ready to apply on next reboot

          Default    Current    Pending
 Table    Length     Length     Length
 ---------------------------------
 1            64         64         64
 2            48         48         63*
 3            46         46         62*
 4            44         44         32*
 5            40         40         31*
 6            36         36         28*

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

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Selecting the system profile

System profiles are applicable to the 6400 Switch Series.

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

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

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

See also System profile commands.

Procedure

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

Examples

Selecting the `v2-Aggregation-High-Bandwidth` profile and then rebooting the system:

```
switch(config)# profile v2-Aggregation-High-Bandwidth
switch(config)# exit
switch# boot system
switch(config)# The config will be cleared, and the switch will be
    rebooted with the v2-Aggregation-High-Bandwidth profile
Continue(y/n)...
```

Selecting the `default` profile and then rebooting the system:

```
switch(config)# profile default
switch(config)# exit
switch# boot system
switch(config)# The config will be cleared, and the switch will be
    rebooted with the Default profile
Continue(y/n)...
```

About 6400 Switch Series module versions and the default system profile

The 6400 Switch Series adds support for V2 modules as of AOS-CX software version 10.10. Prior AOS-CX software versions only support 6400 Series Switches V1 modules.

V1 and V2 modules are identified as follows:

- V1 modules model numbers end with the letter A or B.
- V2 modules model numbers end with the letter C.

The default system profile is decided as follows:

- A 6400 Switch Series V1 chassis uses the `default` system profile as the default. This means that an existing V1 chassis continues to work with existing modules without requiring a configuration change or chassis reboot.
- A 6400 Switch Series V2 chassis uses the `v2-default` system profile as the default. This means that a V2 chassis containing all-V2 modules will work with without requiring a configuration change or chassis reboot.
- A V1 or V2 6400 Switch Series chassis can be configured to use any profile provided that the installed modules support the selected profile.
- In the special case where you run pre-10.10 software on a V2 6400 Switch Series chassis (which means that all modules must be V1) and you then upgrade the software to 10.10 or greater, the V2 6400 Switch Series chassis automatically selects the `default` system profile and then triggers a reboot cycle for the configuration to take effect.

System profile commands

profile

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

Description

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

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

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

Profile names	Description
default	Selects the original default. v1 and v2 modules supported.
v2-default	(The default.) Selects the v2 default. Only v2 modules are supported.
v2-Aggregation-High-Bandwidth	Selects aggregation high bandwidth. Only R0X44C (1G/10G/25G) and R0X45C (40G/100G) v2 modules are supported.
v2-Core-High-Bandwidth	Selects core high bandwidth. Only R0X44C (1G/10G/25G) and R0X45C (40G/100G) v2 modules are supported.
v2-Leaf-Extended-High-Bandwidth	Selects leaf extended high bandwidth. Only R0X44C (1G/10G/25G) and R0X45C (40G/100G) v2 modules are supported.

Examples

Selecting the v2-Aggregation-High-Bandwidth profile and then rebooting the system:

```
switch(config)# profile v2-Aggregation-High-Bandwidth
switch(config)# exit
switch# boot system
switch(config)# The config will be cleared, and the switch will be
    rebooted with the v2-Aggregation-High-Bandwidth profile
Continue(y/n)...
```

Selecting the default profile and then rebooting the system:

```
switch(config)# profile default
switch(config)# exit
switch# boot system
switch(config)# The config will be cleared, and the switch will be
    rebooted with the Default profile
Continue(y/n)...
```

Command History

Release	Modification
10.10	Command introduced on the 6400.

Command Information

Platforms	Command context	Authority
6400	`config`	Administrators or local user group members with execution rights for this command.

show profiles available

```
show profiles available
```

Description

Shows all system profile names available and profile details.

Examples

Showing all available profiles:

```
switch# show profiles available

Available Profiles
------------------
Default              v1 and v2 modules supported
                     32768 L2 entries, 49152 Host entries, 65536 Route entries
v2-Aggregation-      Only R0X44C(1G/10G/25G)& R0X45C(40G/100G)v2 modules supported
  High-Bandwidth     114688 L2 entries, 163840 Host entries, 65536 Route entries
                     enhanced feature set
v2-Core-High-Bandwidth Only R0X44C(1G/10G/25G)& R0X45C(40G/100G)v2 modules supported
                     32768 L2 entries, 65536 Host entries, 630784 Route entries
                     enhanced feature set
v2-Default           Only v2 modules supported (Default)
                     32768 L2 entries, 49152 Host entries, 65536 Route entries
                     enhanced feature set
                     (Default)
v2-Leaf-Extended-    Only R0X44C(1G/10G/25G)& R0X45C(40G/100G)v2 modules supported
  High-Bandwidth     212992 L2 entries, 16384 Host entries, 65536 Route entries
                     enhanced feature set

Note: Not all profiles are supported by all the modules, in order for the profile to
      perform as expected, the profile must be supported by the module.
```

Command History

Release	Modification
10.10	Command introduced on the 6400.

Command Information

Platforms	Command context	Authority
6400	Manager (#)	Administrators or local user group members with execution rights for this command.

show profile current

```
show profile current
```

Description

Shows the current system profile.

Examples

Showing the current profile:

```
switch# show profile current

Current profile
------------------
v2-Aggregation-High-Bandwidth
```

Command History

Release	Modification
10.10	Command introduced on the 6400.

Command Information

Platforms	Command context	Authority
6400	Manager (#)	Administrators or local user group members with execution rights for this command.

Restoring the switch to factory default settings

Prerequisites

You are connected to the switch through its Console port.

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

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

Example

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

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

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10340    0     0  100 10340      0  1329k --:--:-- --:--:-- --:--:-- 1329k
100 10340    0     0  100 10340      0  1313k --:--:-- --:--:-- --:--:-- 1313k
switch#
switch#
switch# erase all zeroize
This will securely erase all customer data and reset the switch
to factory defaults. This will initiate a reboot and render the
switch unavailable until the zeroization is complete.
This should take several minutes to one hour to complete.
Continue (y/n)? y
The system is going down for zeroization.
[  OK  ] Stopped PSPO Module Daemon.
[  OK  ] Stopped AOS-CX Switch Daemon for BCM.
...
[  OK  ] Stopped Remount Root and Kernel File Systems.
[  OK  ] Reached target Shutdown.
reboot: Restarting system
Press Esc for boot options
ServiceOS Information:
    Version:            GT.01.03.0006
    Build Date:         2018-10-30 14:20:44 PDT
    Build ID:           ServiceOS:GT.01.03.0006:8ee0faaa52da:201810301420
    SHA:                xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
...

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

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

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

Boot Profiles:

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

Select profile(primary):

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

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

Extracting Image...
Loading Image...
Done.
kexec_core: Starting new kernel
```

```
System is initializing
fips_post_check[5473]: FIPS_POST: Cryptographic selftest started...SUCCESS
[  OK  ] Started Login banner readiness check.
...
8400X login: admin
Password:

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

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
6300 6400	`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
6300 6400	`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
6300 6400	`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:fefd:e485/64
  Default gateway IPv6        : 2001:db8:0:1::1
  Primary Nameserver          : 2001::1
  Secondary Nameserver        : 2001::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Manager (#)	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}
    [{ <PLAINTXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
no ntp authentication-key <KEY-ID>  {md5 | sha1}
    [{ <PLAINTXT-KEY> [trusted] | ciphertext <ENCRYPTED-KEY> }]
```

Description

Defines an authentication key that is used to secure the exchange with an NTP time server. This command provides protection against accidentally synchronizing to a time source that is not trusted.

The `no` form of this command removes the authentication key.

Parameter	Description
<KEY-ID>	Specifies the authentication key ID. Range: 1 to 65534.
md5	Selects MD5 key encryption.
sha1	Specifies SHA1 key encryption.

Parameter	Description
<PLAINTXT-KEY>	Specifies the plaintext authentication key. Range: 8 to 40 characters. The key may contain printable ASCII characters excluding "#" or be entered in hex. Keys longer than 20 characters are assumed to be hex. To use an ASCII key longer than 20 characters, convert it to hex.
trusted	Specifies that this is a trusted key. When NTP authentication is enabled, the switch only synchronizes with time servers that transmit packets containing a trusted key.
ciphertext *<ENCRYPTED-KEY>*	Specifies the ciphertext authentication key in Base64 format. This is used to restore the NTP authentication key when copying configuration files between switches or when uploading a previously saved configuration. **NOTE:** When the key is not provided on the command line, plaintext key prompting occurs upon pressing Enter, followed by prompting as to whether the key is to be trusted. The entered key characters are masked with asterisks.

Examples

Defining key 10 with MD5 encryption and a provided plaintext trusted key:

```
switch(config)# ntp authentication-key 10 md5 F82#450b trusted
```

Defining key 5 with SHA1 encryption and a prompted plaintext trusted key:

```
switch(config)# ntp authentication-key 5 sha1
Enter the NTP authentication key: *********
Re-Enter the NTP authentication key: *********

Configure the key as trusted (y/n)? y
```

Removing key 10:

```
switch(config)# no ntp authentication-key 10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp disable

```
ntp disable
```

Description

Disables the NTP client on the switch. The NTP client is disabled by default.

Examples

Disabling the NTP client.

```
switch(config)# ntp disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp enable

```
ntp enable
no ntp enable
```

Description

Enables the NTP client on the switch to automatically adjust the local time and date on the switch. The NTP client is disabled by default.

The `no` form of this command disables the NTP client.

Examples

Enabling the NTP client.

```
switch(config)# ntp enable
```

Disabling the NTP client.

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp conductor

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

Description

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

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

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

Examples

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

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

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

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

Command History

Release	Modification
10.08	Inclusive language.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

ntp server

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

Description

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

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

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

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

Usage

For features such as Activate and ZTP, a switch that has a factory default configuration will automatically be configured with pool.ntp.org. NTP server configurations via DHCP options are supported. The DHCP server can be configured with maximum of two NTP server addresses which will be supported on the switch. Only IPV4 addresses are supported.

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

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

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

Examples

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

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

Removing the ntp server pool.ntp.org.

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp trusted-key

```
ntp trusted-key <KEY-ID>
no ntp trusted-key <KEY-ID>
```

Description

Sets a key as trusted. When NTP authentication is enabled, the switch only synchronizes with time servers that transmit packets containing a trusted key.

The `no` form of this command removes the trusted designation from a key.

Parameter	Description
<KEY-ID>	Specifies the identification number of the key to set as trusted. Range: 1 to 65534.

Examples

Defining key 10 as a trusted key.

```
switch(config)# ntp trusted-key 10
```

Removing trusted designation from key 10:

```
switch(config)# no ntp trusted-key 10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ntp vrf

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

Description

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

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

Example

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

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp associations

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

Description

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

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

- POLL: Interval (in seconds) between NTP poll packets. Maximum (1024) reached as server and client sync.
- REACH: 8-bit octal number that displays status of the last eight NTP messages (377 = all messages received).

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

Example

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp authentication-keys

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

Description

Shows the currently defined authentication keys.

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

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp servers

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

Description

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

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

Example

```
switch# show ntp servers
-----------------------------------------------
    NTP SERVER KEYID MINPOLL MAXPOLL OPTION VER
-----------------------------------------------
    192.0.1.18    -      5      10  iburst   3
    192.0.1.19    -      6      10   none    4
    192.0.1.20    -      6       8  burst    3 prefer
-----------------------------------------------
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp statistics

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

Description

Shows global NTP statistics. The following information is displayed:

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

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

Examples

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ntp status

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

Description

Shows the status of NTP on the switch.

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

Examples

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

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

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

Not synchronized with an NTP server.
```

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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 server can be implemented on any VRF using the `telnet server` command. The maximum number of sessions per VRF is five (5).

In the default configuration, Telnet access is disabled.

Telnet commands

show telnet server

```
show telnet server
```

Description

Displays the Telnet server configuration.

Examples

Display the Telnet server configuration on the switch:

```
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
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`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

Displays all active Telnet sessions for the specified VRF or all VRFs. If no VRF is provided, the session on the `default` VRF is shown.

Parameter	Description
`vrf <VRF-NAME>`	Specifies the Telnet sessions for a specific VRF.
`all-vrfs`	Specifies the Telnet sessions for all VRFs

Examples

Display 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
```

Display the Telnet session on all VRFs:

```
switch(config)# show telnet server sessions all-vrfs

TELNET sessions on VRF mgmt:

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

TELNET sessions on VRF default:
    IPv4 TELNET Sessions:
        Server IP        : 20.1.1.1
        Client IP        : 20.1.1.2
        Client Port      : 58837
```

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`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 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.

Examples

Configuring the Telnet server on the `mgmt` VRF:

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

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`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. Set the interface MTU (maximum transmission unit) with the command `mtu`.
3. Review interface configuration settings with the command `show interface`.

Example

On the 6300 switch series:

```
switch(config)# interface 1/1/1
switch(config-if)# mtu 1900
```

On the 6400 switch series:

```
switch(config)# interface 1/3/1
switch(config-if)# mtu 1900
```

Configuring a layer 3 interface

Procedure

1. Change to the interface configuration context for the interface with the command `interface`.
2. 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 on the 6300 Switch Series:

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

This example creates the following configuration on the 6400 Switch Series:

- Configures interface **1/3/1** 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 1/3/1
switch(config-if)# routing
switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/24
switch(config-if)# l3-counters tx
switch(config-if)# l3-counters rx
```

Single source IP address

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

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

Forward error correction

Applies only to the 6300 Switch Series.

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-Aruba 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 Aruba WLAN controllers or former Mobility Access Switch (MAS) products
- End-of-life Aruba 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 eases 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.

The following commands are not supported within the interface context when configuring a persona:

```
aaa authentication port-access dot1x authenticator macsec
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 device-profile <DEVICE-PROFILE-NAME>
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 two 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.

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 an optional argument, required only if the persona is not one of the predefined names (neither **uplink** nor **access**).

For information on this feature, see the related video on the [Aruba AirHeads Broadcasting Channel](#).

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 custom mypersona 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 mypersona attach
switch(config-if)# exit
```

Interface commands

allow-unsupported-transceiver

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

Description

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

The following models will enable unsupported transceivers for speeds up to 100G when running AOS-CX 10.10 or later:

- 6300 Series Switches—Up to 50G
- 6400 Series Switches—Up to 100G

As of AOS-CX 10.06.0100, this command is enabled by default, allowing the use of third party transceiver products without adding the command in the configuration. Disabling this command with the `no` form will now disable the command in the running and stored configurations.

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

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

Usage

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

Examples

Allowing unsupported transceivers with follow-up confirmation:

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

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

Allowing unsupported transceivers with confirmation in command syntax:

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

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

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

Disabling unsupported transceiver logging:

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

Disallowing unsupported transceivers with follow-up confirmation:

```
switch(config)# no allow-unsupported-transceiver
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 6300 (up to 50G) and 6400 (up to 100G) series switches in UT mode.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	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

On the 6400 Switch Series, interface identification differs.

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.

energy-efficient-ethernet

```
energy-efficient-ethernet
```

Description

Enables auto-negotiation of Energy-Efficient Ethernet (EEE) on an interface. EEE Negotiation is established only on auto-link negotiation with supported link partners.

Examples

Configuring an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# energy-efficient-ethernet
```

Disabling Energy Efficient Ethernet on an interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no energy-efficient-ethernet
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

error-control

Applies only to the Aruba 6300 Switch Series.

```
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 25G and 100G transceivers. 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. FEC mode is presented as a commented line in the configuration shown with the `show run` command.

Parameter	Description
`auto`	Use the transceiver default.
`none`	Do not use any FEC.
`base-r-fec`	Use IEEE Clause 74 BASE-R (Firecode) FEC.
`rs-fec`	Use IEEE Clause 91 RS (Reed-Solomon) FEC.

Command History

Release	Modification
10.08.1021	Command introduced

Command Information

Platforms	Command context	Authority
6300	`config-if`	Administrators or local user group members with execution rights for this command.

flow-control

```
flow-control rxtx
no flow-control rxtx
```

Description

Command `flow-control` enables negotiation of IEEE 802.3x link-level flow control on the current interface. The switch advertises link-level flow control support to the link partner. The final configuration is determined based on the capabilities of both partners.

Each invocation of this command replaces the previous configuration.

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

Parameter	Description
`rxtx`	Enables the ability to honor received and to transmit IEEE 802.3x LLFC pause frames to the remote device.

Usage (flow control)

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

Examples

Enabling support for RXTX flow control:

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

Disabling support for RXTX flow control:

```
switch(config)# interface 1/1/1
switch(config-if)# no flow-control rxtx
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

interface

`interface <PORT-NUM>`

Description

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

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

Examples

On the 6400 Switch Series, interface identification differs.

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
6300 6400	`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. Range: 2 to 4094

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 <IPV4-ADDR>/<MASK> [secondary]
no ip address <IPV4-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
`<IPV4-ADDR>`	Specifies an IP address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255. You can remove leading zeros. For example, the address `192.169.005.100` becomes `192.168.5.100`.
`<MASK>`	Specifies the number of bits in the address mask in CIDR format (`x`), where `x` is a decimal number from 0 to 128.
`secondary`	Specifies a secondary IP address.

Examples

On the 6400 Switch Series, interface identification differs.

Creating a layer 3 interface setting its IP address to **192.168.100.1** with a mask of **24** bits.

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

The `no` form of this command sets the IP MTU to the default value 1500. This command is only allowed when routing is enabled on the interface.

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

Examples

Setting the IP MTU to 576 bytes:

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

Setting the IP MTU to the default value:

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

Setting the IP MTU value on a subinterface:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip mtu 6000
```

Usage

The IP MTU value for subinterface must be less than or equal to the parent MTU for the subinterface. The subinterface uses its IP MTU value and not the parent IP MTU value.

Command History

Release	Modification
10.08	Subinterface support added.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if`
	`config-if-vlan`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip source-interface

```
ip source-interface {sflow |  tftp |  radius | tacacs | ntp | syslog | ubt | dhcp-relay |
simplivity | dns | all} {interface <IFNAME> | <IPV4-ADDR>} [vrf <VRF-NAME>]
no ip source-interface {sflow |  tftp |  radius | tacacs | ntp | syslog | ubt | dhcp-relay |
simplivity | dns | all} [interface <IFNAME> | <IPV4-ADDR>] [vrf <VRF-NAME>]
```

Description

Sets a single source IP address for a feature on the switch. This ensures that all traffic sent the feature has the same source IP address regardless of how it egresses the switch. You can define a single global address that applies to all supported features, or an individual address for each feature.

This command provides two ways to set the source IP addresses: either by specifying a static IP address, or by using the address assigned to a switch interface. If you define both options, then the static IP address takes precedence.

The `no` form of this command deletes the single source IP address for all supported services, or a specific service.

Parameter	Description
`sflow	tftp	radius	tacacs	ntp	syslog	ubt	dhcp-relay	simplivity	dns	all`	Sets a single source IP address for a specific service. The `all` option sets a global address that applies to all protocols that do not have an address set. For DHCP relay, the address is used as both the source IP and GIADDR.
`interface <IFNAME>`	Specifies the name of the interface from which the specified service obtains its source IP address. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.
`<IPV4-ADDR>`	Specifies the source IP address to use for the specified service. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the `default` VRF, if the `vrf` option is not used). Specify the address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.
`vrf <VRF-NAME>`	Specifies the name of a VRF.

Examples

Setting the IPv4 address `10.10.10.5` as the global single source address:

```
switch# config
switch(config)# ip source-interface all 10.10.10.5
```

Setting the secondary IPv4 address `10.10.10.5` on interface `1/1/1` as the global single source address. (On the 6400 Switch Series, interface identification differs.)

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

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.

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 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 protocols, or a specific protocol.

Parameter	Description
`sflow	tftp	radius	tacacs	ntp	syslog	ubt	dhcp-relay	simplivity	dns	all`	Sets a single source IP 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 IP address.

Parameter	Description
`<IPV6-ADDR>`	Specifies the source IP address to use for the specified protocol. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the `default` VRF, if the `vrf` option is not used). Specify the IP address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.
`vrf <VRF-NAME>`	Specifies the name of the VRF from which the specified protocol sets its source IP address.

Examples

Configuring the IPv6 address `2001:DB8::1` as the global single source address:

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

Stop the source IP address from using the IP address on interface **1/1/1** on VRF `one`.

```
switch(config)# no ip source-interface all interface 1/1/1 vrf one
```

Clear the source IP address `2001:DB8::1`.

```
switch(config)# no ip source-interface all 2001:DB8::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

---

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 the 6300 Switch Series:

```
switch(config)# interface 1/1/1
switch(config-if)# routing
switch(config-if)# l3-counters
```

On the 6400 Switch Series:

```
switch(config)# interface 1/3/1
switch(config-if)# routing
switch(config-if)# l3-counters
```

Enabling layer 3 transmit counters on subinterfaces

On the 6300 Switch Series:

```
switch(config)# interface 1/1/1.10
switch(config-subif)# routing
switch(config-subif)# l3-counters tx
```

On the 6400 Switch Series:

```
switch(config)# interface 1/3/1.10
switch(config-subif)# routing
switch(config-subif)# l3-counters tx
```

Command History

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

Command Information

Platforms	Command context	Authority
6300 6400	`config-if` `config-subif`	Administrators or local user group members with execution rights for this command.

mtu

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

Description

Sets the MTU (maximum transmission unit) for an interface. This defines the maximum size of a layer 2 (Ethernet) frame. Frames larger than the MTU (1500 bytes by default) are dropped and cause an ICMP fragmentation-needed message to be sent back to the originator.

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

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

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

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

Examples

On the 6400 Switch Series, interface identification differs.

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

persona

```
persona {access | uplink | custom <PERSONA-NAME>} [copy | attach]
no persona {access | uplink | custom <PERSONA-NAME>} [copy | attach]
```

Description

Associates one of three persona types with an interface to classify the purpose or role of an interface. On the 10000 Switch Series, "access" persona ports are typically connected to workloads / VMs, and the "uplink" (fabric) persona ports are connected to the core / spine.

The `no` form of this command removes the interface persona.

Parameter	Description
`access`	Selects the **access** persona type.
`uplink`	Selects the **uplink** persona type.
`custom <PERSONA-NAME>`	Selects the **custom** persona type with a user-provided name. Range: 1 to 64 printable ASCII characters including space.
`copy`	Specifies the mode: copies settings from the persona interface of the same name.
`attach`	Specifies the mode: attaches the specified interface to the persona interface of the same name.

Usage

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

- When a mode is specified, it should match an interface created with the command interface persona *<PERSONA-NAME>*. The only exception to this rule is when the mode is set to `attach` and the persona does not already exist.
- The mode is only available to be configured for an interface that meets the following conditions:
  - IS a physical interface
  - IS NOT a LAG member
  - IS NOT a persona interface

Examples

Configuring an access persona:

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

Configuring an uplink persona:

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

Configuring a custom persona named "mypersona":

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

Removing the persona setting.

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

Copying a predefined persona name configuration to an interface:

1. Configuring the interface persona:

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

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

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

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

1. Configuring an interface persona named "mypersona":

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

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

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

Command History

Release	Modification
10.10	Added optional parameters: attach, copy.
10.09	Command introduced.

Command Information

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

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 disabled on all interfaces.

The `no` form of this command disables routing support on an interface, creating a L2 (layer 2) interface.

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
6300 6400	`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 | extended [non-zero] [human-
readable] | [human-readable]]
show interface [lag | loopback | tunnel | vlan ] [<ID>] [brief | physical]
show interface lag [<LAG-ID>] [extended [non-zero]]
```

Description

Shows active configurations and operational status information for interfaces.

Parameter	Description
`<IFNAME>`	Specifies a interface name.
`<IFRANGE>`	Specifies the port identifier range.
`brief`	Shows brief info in tabular format.
`physical`	Shows the physical connection info in tabular format.
`extended`	Shows additional statistics.
`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.
`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
 Energy-Efficient Ethernet is enabledMDI mode: MDIX
 L3 Counters: Rx Enabled, Tx Enabled
 Rate collection interval: 300 seconds

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

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

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

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

Interface 1/1/1 is up
 ...
 Auto-negotiation is on with downshift active
```

Showing information when the interface is currently linked with energy-efficient-ethernet negotiated:

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


Interface 1/1/1 is up
 ...
 Energy-Efficient Ethernet is enabled and active
```

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

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

Interface 1/1/1 is down
 Admin state is up
 State information: Disabled by VSX
 Link state: down for 3 days (since Tue Mar 16 05:20:47 UTC 2021)
 Link transitions: 0
 Description:

 Hardware: Ethernet, MAC Address: 04:09:73:62:90:e7
 MTU 1500
 Type SFP+DAC3
 Full-duplex
 qos trust none
 Speed 0 Mb/s
 Auto-negotiation is off
 Flow-control: off
 Error-control: off
 VLAN Mode: native-untagged
 Native VLAN: 1
 Allowed VLAN List: 1502-1505
 Rate collection interval: 300 seconds


 Rate                    RX                  TX          Total (RX+TX)
 --------------- -------------------- -------------------- --------------------
 Mbits / sec             0.00                0.00                0.00
 KPkts / sec             0.00                0.00                0.00
   Unicast               0.00                0.00                0.00
   Multicast             0.00                0.00                0.00
   Broadcast             0.00                0.00                0.00
 Utilization             0.00                0.00                0.00

 Statistic               RX                  TX                 Total
 --------------- -------------------- -------------------- --------------------
 Packets                 0                   0                   0
   Unicast               0                   0                   0
   Multicast             0                   0                   0
   Broadcast             0                   0                   0
 Bytes                   0                   0                   0
 Jumbos                  0                   0                   0
 Dropped                 0                   0                   0
 Pause Frames            0                   0                   0
 Errors                  0                   0                   0
   CRC/FCS               0                   n/a                 0
   Collision             n/a                 0                   0
   Runts                 0                   n/a                 0
   Giants                0                   n/a                 0
```

Showing information when the interface is configured with EEE and the EEE has auto-negotiated:

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

----------------------------------------------------------------------------------
-------------------------------------------------------------
                         Link    Admin         Speed          Flow-Control
   EEE       PoE Power                         Port
Port       Type          Status  Config   Status | Config   Status | Config
Status | Config  (Watts)   State Information  Description
----------------------------------------------------------------------------------
-------------------------------------------------------------
1/1/1      1GbT            up      up       1G      auto      off     off     on
     on        --       10M/100M/1G          --
```

Showing the output in human-readable format:

> In the 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
...
```

Command History

Release	Modification
10.10	Added `human-readable` parameter.
10.07 or earlier	--

Command Information

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

show interface dom

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

On the 6400 Switch Series, interface identification differs.

```
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 energy-efficient ethernet

```
show interface [<IFNAME>|<IFRANGE>] energy-efficient-ethernet
```

Description

Displays Energy-Efficient Ethernet information for the interface.

Parameter	Description
<IFNAME>	Specifies the name of an interface on the switch. Use the format `member/slot/port` (for example, `1/1/1`).
<IFRANGE>	Specifies the port identifier range of an interface on the switch. Use the format `member/slot/port` (for example, `1/1/1`).

Example

The following example shows when the interfaces are Energy-Efficient Ethernet capable

```
switch# show interface energy-efficient-ethernet
-----------------------------------------------------------------
Port    Enabled    Negotiated    Speed      TX Wake     RX Wake
                                 (MB/s)     Time(us)    Time (us)
-----------------------------------------------------------------
1/1/1   no         no            --         --          --
1/1/2   yes        yes           100        36          36
1/1/3   yes        yes           1000       17          17
1/1/4   no         no            --         --          --
1/1/5   yes        no            1000       --          --
```

The following example shows when the interface is not Energy-Efficient Ethernet capable :

```
switch# show interface 1/1/1 energy-efficient-ethernet
    Port 1/1/1 does not support Energy-Efficient-Ethernet
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show interface flow-control

`show interface [<IFNNAME>|<IFRANGE>] flow-control [detail]`

Description

Shows the flow control configuration, status, and statistics of the specified interface for interfaces on which flow control is enabled.

> If `detail` is not specified, this command shows a summary of all flow controlled interfaces with one interface per line. If `detail` is specified, this command shows flow control detailed statistics.

> As of AOS-CX 10.10, the separate `show flow-control` command has been removed, with it being effectively replaced by this command.

Parameter	Description
`<IFNNAME>|<IFRANGE>`	Specifies the interface (port) name or range. When no interface range is specified, only interfaces with flow control enabled in the configuration or status are shown.
`detail`	Shows detailed information.

Examples

Showing summary flow control information:

```
switch# show interface flow-control

---------- ------------------------------------
Port       Flow
           Control
---------- ------------------------------------
1/1/1      config: llfc rx
           status: llfc rx
1/1/2      config: llfc rx
           status: none
```

Showing summary flow control information with PFC:

```
switch# show interface flow-control

---------- ------------------------------------
Port       Flow
```

```
           Control
----------- ------------------------------------
1/1/1      config: pfc rxtx-1,2
           status: pfc rxtx-1,2
1/1/2      config: pfc rxtx-5
           status: none
```

Showing summary flow control information with PFC:

```
switch# show interface flow-control
 Flow Control Watchdog Settings
   Trigger Timeout:  100 milliseconds
   Resume Time:      100 milliseconds


----------- ------------------------------------ ------------- --------
Port        Flow                                 Watchdog      Watchdog
            Control                              Status        Timeouts
----------- ------------------------------------ ------------- --------
1/1/1       config: llfc rx
            status: llfc rx
1/1/2       config: llfc rx                      incompatible         0
            status: llfc rx
1/1/10      config: pfc rxtx-1,2                 enabled           1234
            status: pfc rxtx-1,2
1/1/12      config: pfc rxtx-1,2                 error                0
            status: pfc rxtx-1,2
1/1/32:4    config: pfc rxtx-5
            status: pfc rxtx-5
```

Showing summary flow control information where the configuration does not match status due to a reboot required to apply PFC configuration in hardware:

```
switch# show interface flow-control

 Flow Control Watchdog Settings
   Trigger Timeout:  100 milliseconds (actual: not applied)
   Resume Time:      100 milliseconds (actual: not applied)


----------- ------------------------------------ ------------- --------
Port        Flow                                 Watchdog      Watchdog
            Control                              Status        Timeouts
----------- ------------------------------------ ------------- --------
1/1/1       config: llfc rx
            status: llfc rx
1/1/2       config: llfc rx                      incompatible         0
            status: llfc rx
1/1/10      config: pfc rxtx-1,2                 pending           1234
            status: none
1/1/12      config: pfc rxtx-1,2                 pending              0
            status: none
1/1/32:4    config: pfc rxtx-5
            status: none
```

Showing detailed flow control information with RX flow control enabled:

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

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

Showing detailed flow control information with RX flow control enabled:

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

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

Showing detailed flow control information with RXTX flow control enabled:

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

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

Showing detailed flow control information with PFC enabled:

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

 Statistics                            RX                   TX
 ------------------- -------------------- --------------------
 Priority 0 Pauses                       0                    0
 Priority 1 Pauses                       0                    0
 Priority 2 Pauses                       0                    0
 Priority 3 Pauses                       0                    0
 Priority 4 Pauses                       0                    0
 Priority 5 Pauses                       0                    0
 Priority 6 Pauses                       0                    0
```

```
Priority 7 Pauses                                0                    0
Total Pause Frames                               0                    0
```

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

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

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

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

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

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

 Queue          Watchdog Timeouts
 ------------ -----------------
 Queue 0                      0
 Queue 1                      0
 Queue 2                      0
 Queue 3                      0
 Queue 4                      0
 Queue 5                      0
 Queue 6                      0
 Queue 7                      0
```

Showing detailed flow control information when flow control watchdog is enabled in the configuration but it could not be applied because the configured flow control mode is not compatible with watchdog:

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

Showing detailed flow control information when flow control watchdog is enabled in the configuration but could not be applied because a compatible flow control mode first requires a reboot:

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

Command History

Release	Modification
10.10	Examples updated with new and changed output elements.
10.08	Command introduced.

Command Information

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

show interface statistics

```
show interface [<IFNAME>|<IFRANGE>] statistics [non-zero] [human-readable]
show interface [<IFNAME>|<IFRANGE>] error-statistics [non-zero] [human-readable]
show interface lag [<LAG-ID>] statistics [non-zero] [human-readable]
show interface lag [<LAG-ID>] error-statistics [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
`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 Pause
----------------------------------------------------------------------------------------------------------------------------------
1/1/1                2727136   1975        0         17796     195         0         82            1788          96            54            0         0
1/1/10               0         0           0         0         0           0         0             0             0             0             0         0
1/1/11               0         0           0         0         0           0         0             0             0             0             0         0
1/1/12               0         0           0         0         0           0         0             0             0             0             0         0
...
1/1/30     - lag1    0         0           0         11271     92          0         0             0             0             51            0         0
1/1/31     - lag2    2360      25          50        2732119   2040        0         0             0             178           1839          0         0
1/1/32     - lag2    0         0           0         11373     93          0         0             0             0             51            0         0
vlan1                0         0           0         0         0           0         0             0             0             0             0         0
```

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

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

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

```
show interface statistics human-readable
----------------------------------------------------------------------------------------------------------------------------------
Interface            RX Bytes  RX Pkts  RX Drops  TX Bytes  TX Pkts  TX Drops  RX Bcast  RX Mcast  TX Bcast  TX Mcast  RX Pause  TX Pause
----------------------------------------------------------------------------------------------------------------------------------
1/1/1                744M      577K     0         745M      578K     0         0         0         73        287       0         0
1/1/2                474M      367K     0         475M      369K     0         0         0         73        288       0         0
1/1/3                0         0        0         0         0        0         0         0         0         0         0         0
```

Showing statistics of a single interfaces:

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

Showing statistics of all members of a LAG interface:

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

Showing error statistics of all interfaces:

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

Command History

Release	Modification
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

On the 6400 Switch Series, interface identification differs.

Showing summary transceiver information with identification of unsupported transceivers:

```
switch(config)# show interface transceiver
-------------------------------------------------------------------------
Port       Type          Product        Serial         Part
                         Number         Number         Number
-------------------------------------------------------------------------
1/1/1      SFP+SR        J9150A         MYxxxxxxxx     1990-3657
1/1/2      SFP+ER*       --             --             --
1/2/1      QSFP+SR4      JH233A         MYxxxxxxxx     2005-1234
1/2/2      QSFP+ER4*     --             --             --
1/3/1      SFP28DAC3     844477-B21     MYxxxxxxxx     77fc-7ce7

* unsupported transceiver
```

Showing detailed transceiver information:

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

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

  Recent Alarms :
    Rx power low alarm
    Rx power low warning

  Recent Errors :
    Rx loss of signal

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

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

```
   Part Number         : 2005-1234

Status
   Temperature : 44.46C
   Voltage     : 3.30V


   -------------------------------------------------
            Tx Bias  Rx Power     Tx Power
   Channel#  (mA)     (mW/dBm)     (mW/dBm)
   -------------------------------------------------
   1        6.12     0.00, -inf   0.63, -1.95
   2        6.04     0.00, -inf   0.63, -2.00
   3        6.51     0.00, -inf   0.60, -2.16
   4        6.19     0.00, -inf   0.63, -1.94

   Recent Alarms :
     Channel 1 :
        Rx power low alarm
        Rx power low warning
     Channel 2 :
        Rx power low alarm
        Rx power low warning
     Channel 3 :
        Rx power low alarm
        Rx power low warning
     Channel 4 :
        Rx power low alarm
        Rx power low warning

   Recent Errors :
     Channel 1 :
        Rx Loss of Signal
     Channel 2 :
        Rx Loss of Signal
     Channel 3 :
        Rx Loss of Signal
     Channel 4 :
        Rx Loss of Signal

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

Transceiver in 1/3/1
   Interface Name    : 1/3/1
   Type              : SFP28DAC3
   Connector Type    : Copper Pigtail
   Transfer Distance : 0.00km (SMF), 0m (OM1), 0m (OM2), 0m (OM3)
   Diagnostic Support : None
   Product Number    : 844477-B21
   Serial Number     : MYxxxxxxx
   Part Number       : 77fc-7ce7
```

Showing detailed transceiver information with identification of unsupported transceivers:

```
switch# show interface transceiver detail
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:
  Rx loss of signal
```

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 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> [vsx-peer]
```

Description

Shows status and configuration information for an IPv4 interface.

Parameter	Description
`<INTERFACE-ID>`	Specifies the name of an interface. Format: `member/slot/port`.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

```
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
 IPv4 address 192.168.1.1/24
 MTU 1500
 RX
         0 packets, 0 bytes
 TX
         0 packets, 0 bytes
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip source-interface

```
show ip source-interface {sflow |  tftp |  radius | tacacs | all} [vrf <VRF-NAME>]
    [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

On the 6400 Switch Series, interface identification differs.

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

On the 6400 Switch Series, interface identification differs.

```
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 unicast reverse path forwarding: none
 IPv6 load sharing: none
 RX
        0 packets, 0 bytes
 TX
        0 packets, 0 bytes
```

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 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

On the 6400 Switch Series, interface identification differs.

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.

speed

```
speed {SPEED-DUPLEX | AUTO <SPEED>}
no speed
```

Description

Configures the link speed, duplex, and auto-negotiation settings for an interface. Auto-negotiating speed and duplex during link establishment is the default.

The no form of this command removes the configurations and returns to the default. s

Parameter	Description
<SPEED-DUPLEX>	Configures interface speed, duplex, and auto-negotiation.
10-full	10 Mbps, full duplex, no auto-negotiation.
10-half	10 Mbps, half duplex, no auto-negotiation.
100-full	100 Mbps, full duplex, no auto-negotiation.
100-half	100 Mbps, half duplex, no auto-negotiation.
1000-full	1000 Mbps, full duplex, no auto-negotiation.
<AUTO>	Auto-negotiate speed and duplex. More than one speed can be set at a time.
10m	Allow interface to link at 10 Mbps.
100m	Allow interface to link at 100 Mbps.
1g	Allow interface to link at 1 Gbps.
2.5g	Allow interface to link at 2.5 Gbps.
5g	Allow interface to link at 5 Gbps.
10g	Allow interface to link at 10 Gbps.
25g	Allow interface to link at 25 Gbps.
40g	Allow interface to link at 40 Gbps.
50g	Allow interface to link at 50 Gbps.
100g	Allow interface to link at 100 Gbps.

Usage

- 6300, 6400 SmartRate or Multigig ports configured to 100-full (without autonegotiation) operate in MDIx mode. If connected to another device in MDIX mode, a crossover cable must be used to link up.
- Configured speeds that are not compatible with the current hardware are ignored and the best compatible speeds are used instead.
- For compatibility with devices that do not auto-negotiate, the specific speed and duplex settings can be configured with this command.
- Some interface and transceiver types require specific settings for speed, duplex, and auto-negotiation. Settings configured with this command are ignored if they cannot be applied legally.
- When auto-negotiation is enabled, an optional list of speeds can be configured and the interface will only advertise the speeds in the list instead of all supported speeds.

Examples

Configure an interface to operate at a fixed speed of 1000 Mbps with full duplex and no auto-negotiation:

```
switch(config)# interface 1/1/1
switch(config-if)# speed 1000-full
```

Configure an interface to use default settings for speed, duplex, and auto-negotiation:

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

Configure an interface to advertise only 1 Gbps and 10 Gbps speeds:

```
switch(config)# interface 1/1/1
switch(config-if)# speed auto 1g 10g
```

Command History

Release	Modification
10.09.0001	Speeds not supported by hardware hidden by CLI.
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	config-if	Administrators or local user group members with execution rights for this command.

system interface-group

This command only applies to the following modules:

- R0X44A Aruba 6400 48p 10G/25G SFP28 Module

- R0X44C Aruba 6400 48p 1G/10G/25G SFP28 v2 Module

```
system interface-group <GROUP> line-module <SLOT-ID> speed <SPEED>
no system interface-group <GROUP> line-module <SLOT-ID>
```

Description

Configures speed for an interface group. After changing group speed, only transceivers compatible with the new speed will be enabled.

- R0X44C (version 2) is the only module that can apply 50G speed as an option. If the command is attempted to any other type of module, the command is ignored.

- 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 interface group to configure.
`<SPEED>`	Configures transceiver speed (10g, 25g or 50g) for a group. Default is 25g (see the _Transceiver Guide_ for further detail). On 6400 Switch Series: ■ 25g allows transceivers up to 25Gbps. ■ 50g allows 50Gbps transceivers and DACs on the R0X44C version 2 module. This command is ignored on any other type of module (including R0X44A version 1).
`<SLOT-ID>`	Specifies 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 or later	Command introduced

Command Information

Platforms	Command context	Authority
6400	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

A subinterface is a virtual interface created by dividing one physical interface into multiple logical interfaces. Subinterfaces use the parent physical interface for sending and receiving data.

Supported features

The following features are supported on L3 subinterfaces:

- RoP, L3 LAG and Hydra interface (split cable) support
- IPv4/IPv6 addressing
- ARP/ND
- Static unicast routing (IPv4/IPv6)
- Unicast routing (IPv4/IPv6) - OSPF and VRRP
- Unicast routing (IPv4/IPv6) - BGP and IVRL
- IPv4/IPv6 multicast routing (IGMP and PIM)
- Ingress ACLs and Ingress Policies
- MTU (maximum transmission unit)
- L3 counters
- VSX keep alive links
- SNMP read
- REST support

Configuring subinterfaces

- Subinterfaces can be configured for physical ports, split children of physical ports and L3 LAG interfaces.
- An L3 interface with subinterfaces must be attached to the default VRF.
- Subinterfaces on multiple ports can be assigned the same VLAN ID (there is no bridging between subinterfaces or between subinterfaces and SVIs). Each subinterface is considered to be in a separate bridge domain.
- The parent interface's IP MTU (maximum transmission unit) can be equal to or greater than the value configured on the child subinterface.

Procedure

One router with one physical interface needs to be connected to two IP networks:

1. Create two subinterfaces within the physical interface.
2. Assign each subinterface an IP address within each subnet.
3. Route packets between the two subnets.

Limitations

- Subinterfaces can only be configured on L3 ports with routing enabled.
- A subinterface cannot be a member of a LAG.
- An L3 interface with subinterfaces cannot be a member of a LAG.
- An L3 interface with subinterfaces cannot be used for L3 services (for example IP address configuration is not supported on an L3 interface if the interface is configured with subinterfaces).
- On physical interfaces, each subinterface must have a unique encapsulation ID.

> Subinterface applications use VLAN context group selectors because they are matched on the subinterface's internal VLAN number in hardware. For example, if one of the "Ingress VLAN" context group selectors is allocated (due to one or more MAC ACLs applied to VLANs on ingress), it can be shared with one or more MAC ACLs applied to subinterfaces on ingress.

Subinterface in a router-on-a-stick deployment
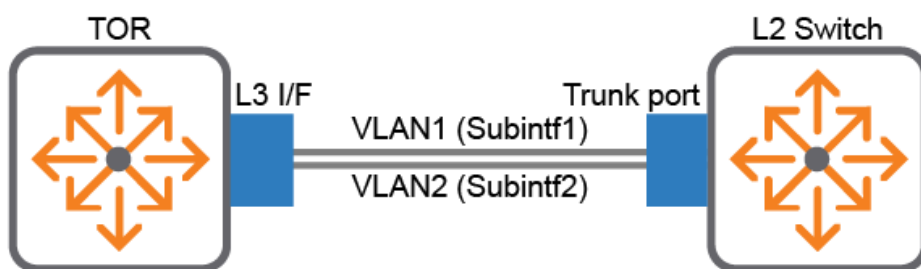
- Top-of-rack switch/router with an L3 interface connected to the trunk port of an L2 switch.
- Routing tables configured to forward outgoing traffic through a subinterface while applying a VLAN ID tag.
- All outgoing traffic from the L3 interface is tagged with a VLAN ID which enables the switch to forward traffic through different VLANs.

Subinterface commands

encapsulation dot1q

```
encapsulation dot1q <VLAN-ID>
no encapsulation dot1q <VLAN-ID>
```

Description

Configures 802.1Q encapsulation on a subinterface.

The `no` form of this command removes 802.1Q encapsulation on a subinterface.

Parameter	Description
`<VLAN-ID>`	Specifies encapsulation VLAN ID. Range 1 to 4094.

Usage

- Associates an 802.1Q VLAN ID with a subinterface.

Examples

Configuring 802.1Q encapsulation on a subinterface:

```
switch(config)# interface 1/1/1.201
switch(config-subif)# encapsulation dot1q 10
```

Removing 802.1Q encapsulation on a subinterface:

```
switch(config-subif)# no encapsulation dot1q 10
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	`config-subif`	Administrators or local user group members with execution rights for this command.

interface

```
interface <IFNAME>.<ID>
no interface <IFNAME>.<ID>


interface lag <LAGNUM>.<ID>
no interface lag <LAGNUM>.<ID>
```

Description

Creates a subinterface on an L3 interface and enters subinterface configuration mode. The subinterface name consists of the parent interface name (for example, 1/1/1) followed by a period and a unique ID number.

The `no` form of these commands deletes a subinterface from an L3 interface.

Parameter	Description
`<IFNAME>`	Specifies L3 interface name.
`<ID>`	Specifies subinterface ID. Range 1 to 4094.
`<LAGNUM>`	Specifies L3 LAG interface number.

Usage

- To create a LAG subinterface, parent LAG must exist before creating the subinterface.

Examples

Creating a subinterface on L3 interface 1/1/1.201 and entering subinterface configuration mode:

```
switch(config)# interface 1/1/1.201
switch(config-subif)#
```

Deleting subinterface on L3 interface 1/1/1.201:

```
switch(config)# no interface 1/1/1.201
```

Creating a subinterface on an L3 LAG port and entering subinterface configuration mode:

```
switch(config)# interface lag 1.201
switch(config-subif)#
```

Deleting subinterface on an L3 LAG port :

```
switch(config)# no interface lag 1.201
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	config	Administrators or local user group members with execution rights for this command.

show capacities subinterface

```
show capacities subinterface
```

Description

Displays maximum subinterface capacity.

Examples

Showing maximum subinterface capacity:

```
switch# show capacities subinterface

System Capacities: Filter Subinterface
Capacities Name                                                               Value
-----------------------------------------------------------------------------------
Maximum number of LAG subinterfaces for the entire system                       256
Maximum number of LAG members when the LAG has subinterfaces                       4
Maximum number of normal subinterfaces for the entire system                   1024
```

```
Maximum number of subinterface resources for the entire system (normal+(4*LAG) 1024
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show interface

```
show interface <IFNAME>.<ID>
show interface lag <LAGNUM>.<ID>
```

Description

Displays subinterface configuration.

Parameter	Description
<IFNAME>	Specifies L3 interface name.
<ID>	Specifies subinterface ID. Range 1 to 4094.
<LAGNUM>	Specifies L3 LAG interface number.

Examples

Showing subinterface configuration:

```
switch# show interface 1/1/1.201
Interface 1/1/1.201 is down
Admin state is up
State information: Waiting for link
Description:
Hardware: Ethernet, MAC Address: 38:21:c7:5a:80:80
Encapsulation dot1Q ID: 10
Statistic                        RX                   TX                   Total
----------------  --------------------  --------------------  --------------------
L3 Packets                        0                    0                    0
L3 Bytes                          0                    0                    0
```

Showing subinterface LAG configuration:

```
switch# show interface lag1.1
Interface lag1.1 is down
```

```
Admin state is up
Description:
Hardware: Ethernet, MAC Address: 38:21:c7:5a:80:80
Encapsulation dot1Q ID: 2
Statistic                       RX                   TX                   Total
----------------  --------------------  --------------------  --------------------
L3 Packets                       0                    0                    0
L3 Bytes                         0                    0                    0
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

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 (protocol <ip-addr>)

```
ip source-interface <PROTOCOL> <IP-ADDR> [vrf <VRF-NAME>]
no ip source-interface <PROTOCOL> <IP-ADDR> [vrf <VRF-NAME>]
```

Description

Configures the source-interface IPv4 address to use for the specified protocol. If a VRF is not given, the default VRF applies. If no interface option is given, the device floods through interfaces and VRFs to reach Aruba Central. Whichever reaches Aruba Central will be picked automatically.

The `no` form of this command removes all configurations.

Parameter	Description

<PROTOCOL>	Specifies the protocol to configure.
	`all`
	    Selects all protocols that can be configured by this command.
	`central`
	    Selects Aruba Central.
	`dhcp_relay`
	    Selects DHCP relay.
	`dns`
	    Selects DNS.
	`ntp`
	    Selects NTP.
	`radius`
	    Selects radius.
	`sflow`
	    Selects sFLow.

Parameter	Description

	simplivity
	    Selects simplivity.
	syslog
	    Selects syslog.
	tacacs
	    Selects TACACS.
	tftp
	    Selects TFTP.

<IP-ADDR>	Specifies the IPv4 address.
vrf *<VRF-NAME>*	Specifies the VRF name.

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip source-interface

```
ip source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]
no ip source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]
```

Description

Configures the IPv4 source-interface interface to use for the specified protocol. If a VRF is not given, the default VRF applies.

The `no` form of this command removes the specified configuration.

Parameter	Description

`<PROTOCOL>`	Specifies the protocol to configure. `all`
	   Selects all protocols that can be configured by this command.
	`central`
	   Selects Aruba Central.
	`dhcp_relay`
	   Selects DHCP relay.
	`dns`
	   Selects DNS.
	`ntp`
	   Selects NTP.
	`radius`
	   Selects radius.
	`sflow`
	   Selects sFLow.
	`syslog`
	   Selects syslog.
	`tacacs`
	   Selects TACACS.
	`tftp`
	   Selects TFTP.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.
<IFNAME>	Specifies the interface name.

Examples

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

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

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

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ipv6 source-interface

```
ipv6 source-interface <PROTOCOL> <IPV6-ADDR> [vrf <VRF-NAME>]
no source-interface <PROTOCOL> <IPV6-ADDR> [vrf <VRF-NAME>]
```

Description

Configures the source-interface IPv6 address 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 protocol configuration.

Parameter	Description
<PROTOCOL>	Specifies the protocol to configure. ■ all:Selects all protocols supported by this command. ■ central:Selects Aruba Central. ■ ntp:Selects NTP. ■ radius:Selects radius. ■ sflow:Selects sFLow. ■ syslog:Selects syslog. ■ tacacs:Selects TACACS. ■ tftp:Selects TFTP.
<IPV6-ADDR>	Specifies the IPv6 address.
vrf *<VRF-NAME>*	Specifies the VRF name.

Examples

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
10.07 or earlier	--

Command Information

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

ipv6 source-interface

```
ipv6 source-interface <PROTOCOL> interface <IFNAME> [vrf <VRF-NAME>]
no ipv6 source-interface <PROTOCOL> 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 all protocols supported by this command.
	`central`
	Selects Aruba Central.
	`ntp`
	Selects NTP.
	`radius`
	Selects radius.
	`sflow`
	Selects sFLow.
	`syslog`
	Selects syslog.
	`tacacs`
	Selects TACACS.
	`tftp`
	SelectsTFTP.

`<IFNAME>`	Specifies the interface name.
`vrf <VRF-NAME>`	Specifies the VRF name.

`<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
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip source-interface

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

Description

Displays the source interface information for all VRFs or a specific VRF.

If a VRF is not specified, the default is displayed.

Parameter	Description

`<PROTOCOL>`	Specifies the protocol to show.
	`all`
	    Shows the source interface configuration for all other protocols.
	`central`
	    Shows the source interface configuration for Aruba Central.
	`dhcp relay`
	    Shows the source interface configuration for DHCP relay.
	`dns`
	    Shows the source interface configuration for DNS.
	`ntp`
	    Shows the source interface configuration for NTP.
	`radius`
	    Shows the source interface configuration for radius.
	`sflow`
	    Shows the source interface configuration for sFLow.
	`syslog`
	    Shows the source interface configuration for syslog.
	`tacacs`
	    Shows the source interface configuration for TACACS.
	`tftp`
	    Shows the source interface configuration for TFTP.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF name.
all-vrfs	Shows the source interface configuration for all VRFs.

Examples

Displaying all source-interface protocol configurations for VRF red:

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

Displaying all source-interface protocol configurations for default VRF:

```
switch# show ip source-interface all
Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP              VRF
------------------------------------------------------------------
all                                 1.1.1.1             default
switch#
```

Displaying all source-interface protocol configurations for all VRFs:

```
switch# show ip source-interface all all-vrfs
Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP              VRF
------------------------------------------------------------------
all                                 2.2.2.2             all-vrfs
all                                 1.1.1.1             default
all             1/1/1/1                                 red
switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ipv6 source-interface

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

Description

Displays the IPV6 source interface information configured in the router for all VRFs or a specific VRF.

If a VRF is not specified, the default is displayed.

Parameter	Description

`<PROTOCOL>`	Specifies the protocol to show.
	 `all`
	      Shows the source interface configuration for all other protocols.
	 `central`
	      Shows the source interface configuration for Aruba Central.
	 `ntp`
	      Shows the source interface configuration for NTP.
	 `radius`
	      Shows the source interface configuration for radius.
	 `sflow`
	      Shows the source interface configuration for sFLow.
	 `syslog`
	      Shows the source interface configuration for syslog.
	 `tacacs`
	      Shows the source interface configuration for TACACS.
	 `tftp`
	      Shows the source interface configuration for TFTP.

`vrf <VRF-NAME>`	Specifies the VRF name.
`all-vrfs`	Shows the source interface configuration for all VRF.

Examples

Displaying all IPv6 source-interface protocol configurations for default VRF:

```
switch# show ipv6 source-interface all
Source-interface Configuration Information
-------------------------------------------------------------------
Protocol        Src-Interface       Src-IP              VRF
-------------------------------------------------------------------
all                                 1111:2222           default
switch#
```

Displaying all IPv6 source-interface protocol configuration for VRF red:

```
switch# show ipv6 source-interface all vrf red
Source-interface Configuration Information
------------------------------------------------------------------
Protocol        Src-Interface       Src-IP              VRF
------------------------------------------------------------------
all             1/1/1                                   red
switch#
```

Displaying all IPv6 source-interface protocol configurations for all VRFs:

```
switch# show ipv6 source-interface all all-vrfs
Source-interface Configuration Information
----------------------------------------------------------------
Protocol        Src-Interface        Src-IP              VRF
----------------------------------------------------------------
all                                  2.2.2.2:3.3.3.3     all-vrfs
all                                  1.1.1.1:2.2.2.2     default
all             1/1/1                2::2                red
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 running-config

```
show running-config
```

Description

Displays the current running configuration.

Examples

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

Aruba Central is the priority agent. If no command is specified for ip source-interface, Central will choose the command automatically if it is reachable on any of the known ports.

```
switch# show running-config
vrf green
ip source-interface tftp interface 1/1/2 vrf green
ip source-interface radius interface 1/1/2 vrf green
ip source-interface ntp interface 1/1/2 vrf green
ip source-interface tacacs interface 1/1/2 vrf green
ip source-interface dns interface 1/1/2 vrf green
ip source-interface central interface 1/1/2 vrf green
ip source-interface all interface 1/1/2 vrf green
ipv6 source-interface tftp 2222::3333 vrf green
ipv6 source-interface radius 2222::3333 vrf green
ipv6 source-interface ntp 2222::3333 vrf green
ipv6 source-interface tacacs 2222::3333 vrf green
ipv6 source-interface central 2222::3333 vrf green
```

```
ipv6 source-interface all 2222::3333 vrf green
ip source-interface tftp 10.20.3.1
ip source-interface radius 10.20.3.1
ip source-interface ntp 10.20.3.1
ip source-interface tacacs 10.20.3.1
ip source-interface dns 10.20.3.1
ip source-interface central 10.20.3.1
ip source-interface all 10.20.3.1
interface 1/1/1
    no shutdown
    ip address 10.20.3.1/24
interface 1/1/2
    vrf attach green
    ip address 20.1.1.1/24
    ipv6 address 2222::3333/64
interface 1/1/45
    no shutdown
    ip address 100.1.0.1/24
    ipv6 address 1111::2222/64
ip route 100.2.0.0/24 10.20.3.2
switch#
```

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.

> PTP is available on the Aruba 6300 Switch Series.

> If PTP is configured on MACsec-supported ports, the switch can experience higher jitter or lower PTP accuracy.

Precision Time Protocol (PTP) is defined in the IEEE 1588 standard (Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems). PTP synchronizes clocks in packet-based networks that include distributed device clocks of varying precision and stability. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. PTP is currently employed to synchronize financial transactions, mobile phone tower transmissions, and networks that require precise timing but lack access to satellite navigation signals.

PTP clocks

A PTP network consists of PTP-enabled devices and devices that are not using PTP. The PTP-enabled devices typically consist of clock-aware devices such as ordinary clocks (which are usually single-port end-stations) and one or more grandsource clocks, transparent clocks, and boundary clocks (multi-port L2/L3 time-aware devices).

The basic clock node types include:

Grandsource clock—A grandsource clock is the primary source of time for the downstream devices. This is a device with greater clock quality which may have direct access to a reference clock.

Ordinary clock—An ordinary clock is a single port end-station (which can include a GM as the originating PTP time-aware device).

Transparent clock—A transparent clock can have multiple network port connections but it does not act as either a clock-source or a clock-sink. Rather, it updates the correction field within the PTP event messages (`SYNC/FOLLOW_UP`, `DELAY_REQUEST`) to compensate for the transit time delay. Transparent clocks compensate for switch latency and jitter, making network devices appear transparent to other PTP time-aware devices. They help in reducing the end-station time errors and improving synchronization quality. But a transparent clock itself does not synchronize its time. An **End-to-End (E2E) transparent clock** updates the `correctionField` field in the PTP messages with the total time the PTP packet was resident in the network device. This is called resident time correction.

Boundary clock—A boundary clock implements a local PTP clock where one port acts as clock-sink which synchronizes itself with the clock-source while other ports act as clock-source ports to its downstream clock-aware devices. The clock-source port is used to redistribute the clock to another set of clock-sinks. Boundary clocks can also use E2E and can be configured based on the selected PTP profile. The best clock source algorithm is used by the boundary clock to select the best or most precise configured acceptable clock-source clock.

Based on hardware capability, the switch supports either boundary clock, transparent clock, or both modes.

> On the Aruba 6300 Switch Series, boundary clock (BC 1-step E2E) is available only on models R8S89A and R8S90A. All other Aruba 6300 Switch Series models support only transparent clock (TC 1-step E2E).

Best clock-source algorithm

The best clock-source algorithm helps in choosing the source of timing on your network. It runs independently on each clock in a domain. This algorithm specifies the way that a local clock can determine which of all the clocks (including itself) is the best. Since it runs continuously, it continually re-adapts to changes in the network or the clocks.

Each clock sends a message to the network describing its own properties. The best clock-source algorithm running in the clock compares these properties to determine the best clock.

The comparisons of attributes happens with the following precedence :

1. Priority1: user configurable absolute priority
2. ClockClass: Attribute defining a clock's TAI traceability
3. Time Source: Attribute defining the accuracy of a clock
4. Variance: An attribute defining the precision of a clock
5. Priority2: This is a user configurable designation that provides finer grained ordering among otherwise equivalent clocks
6. Clock Identity : A tiebreaker consisting of the MAC address of the clock

In addition to this precedence order, the distance measured by the number of boundary clocks between the local clock and the best clock is used when two Announce messages reflect the same best clock. The distance is indicated in the stepsRemoved field of announce messages.

PTP network diagram

The following diagram illustrates how the various PTP clock nodes are connected and how the timing information flows from the origin to the end-stations to achieve the time synchronization. This diagram depicts the PTP clocks in a source-sink hierarchy.

Figure 1 *Example PTP network with clocks in a source-sink hierarchy*
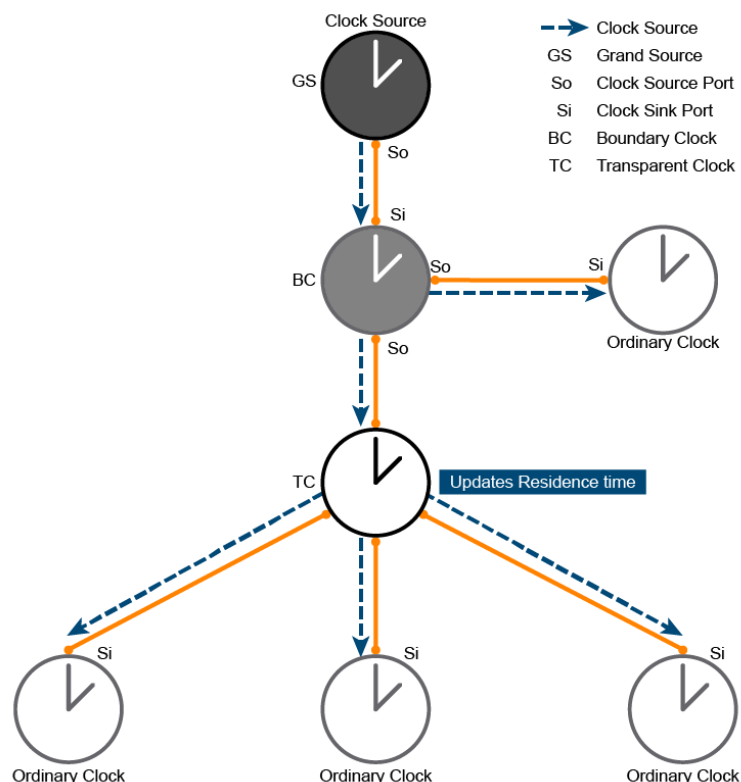
Configuration examples

Configuring an end-to-end transparent clock (TC E2E)

Follow these steps to configure the E2E transparent clock:

1. Configure the mandatory commands:
    a. Configure the PTP mode and the delay mechanism.
    b. Configure the PTP clock-step mode.
    c. Configure the transport protocol.
    d. Configure PTP globally.

```
Switch config:
switch(config)# ptp profile 1588v2
switch(config-ptp)# mode transparent end-to-end
switch(config-ptp)# clock-step one-step
switch(config-ptp)# transport-protocol ethernet
switch(config-ptp)# enable
```

2. Enable PTP on the connected interfaces :

```
switch(config)# int 1/1/1
switch(config-if)# ptp enable
switch(config-if)# int 1/1/2
switch(config-if)# ptp enable
```

Configuring an end-to-end boundary clock (BC E2E)

Follow these steps to configure the end-to-end boundary clock:

1. Create the PTP context using the specified profile.

```
switch(config)# ptp profile 1588v2
switch(config-ptp)#
```

2. Configure the mandatory commands:
    a. Configure the PTP mode.
    b. Configure the PTP clock-step mode.
    c. Configure the transport protocol.
    d. Configure PTP globally.

```
switch(config-ptp)# mode boundary end-to-end
switch(config-ptp)# clock-step one-step
switch(config-ptp)# transport-protocol ethernet
switch(config-ptp)# enable
```

3. Configure the optional commands which participate in the best clock source algorithm:
    a. Configure priority1 value.
    b. Configure priority2 value.

```
switch(config-ptp)# priority1 1
switch(config-ptp)# priority2 10
```

4. Enable PTP on the connected interfaces:

```
switch(config)# int 1/1/1
switch(config-if)# ptp enable
switch(config-if)# int 1/1/2
switch(config-if)# ptp enable
```

5. Optional: changing packet interval rate for various PTP parameters:

```
switch(config-if)# ptp sync-interval 1588v2 1
switch(config-if)# ptp announce-interval 1588v2 -5
switch(config-if)# ptp announce-timeout 1588v2 4
switch(config-if)# ptp delay-req-interval 1588v2 -3
```

PTP over VSF

- When PTP is configured on a Virtual Switch Framework (VSF) stack, each member of the stack calculates the residence-time of the PTP packets.
- All VSF ports are PTP-enabled (by default) when transparent clock is configured for a VSF stack. If the VSF link is up, the interface status is displayed as **Running** in the `show ptp interface brief` command output.

Hardware considerations

The Aruba 6300 Switch Series downlink ports with speed 1G (Smart Rate, non-Smart Rate and XCVR 1G BT) plus 2.5G Smart Rate and 5G Smart Rate have a slightly higher jitter compared to Aruba 6300 Switch Series uplink ports, so the PTP offset of Clients connected on 1G, 2.5G, and 5G downlink ports of the Aruba 6300 Switch Series is slightly higher compared to non-MACsec-supported uplink ports.

Use of third party transceivers may introduce unknown latency and have an effect on the accuracy of PTP deployments.

Configuration recommendations

On the Aruba 6300 Switch Series, boundary clock (BC 1-step E2E) is available only on models R8S89A and R8S90A. All other Aruba 6300 Switch Series models support only transparent clock (TC 1-step E2E).

PTP CoPP class configuration recommendations

Configuration recommendations for a boundary clock

The PTP CoPP class must be adjusted based on the number of clients associated with the boundary clock and the configured packet rate. For example, if there are 1000 clients with a configured packet rate of 2pps,

and a default CoPP limit of 1000, packet drops will be observed. In such instances the CoPP limit should be increased to more than 2000.

The `show copp statistics class ptp` command can be used to monitor whether the CoPP policy must be adjusted. For example:

```
Statistics for CoPP policy 'default':
Class: ptp
Description: Precision Time Protocol (PTP) .
    priority           : 5
    rate (pps)         : 1000
    burst size (pkts)  : 250

    packets passed   : 611153           packets dropped  : 0
```

Increasing the PTP CoPP values may help in scaling the clients but needs to be planned and configured properly so as to not to impact other protocols.

QoS prioritization configuration recommendations for a transparent clock

```
class ip PTP
    10 match udp any any eq 319 count
policy PTP-POL
    10 class ip PTP action local-priority 6
policy test
interface lag 240
    apply policy PTP-POL in
interface 1/1/26
    apply policy PTP-POL in
interface 2/1/26
    apply policy PTP-POL in
```

PTP Event messages carrying a critical timestamp use UDP port 319.

General guidelines for PTP IPv4 multicast

- For IP multicast-based PTP time distribution, it is recommended to use PIM Sparse-Mode.
- When connecting transparent clock (TC) and boundary clock (BC), ensure that the TC becomes the DR by setting the DR priority.
- Ensure the mroutes are programmed on TCs so that there is reachability for PTP streams from the upstream.
- Configure static-igmp groups on TCs if the clients themselves cannot send IGMP joins for the PTP multicast group.
- The `QoS trust dscp` command needs to be explicitly configured on all non-BC switches in the network to ensure that the incoming DSCP value of PTP traffic is honored.

Use cases

Use case: PTP – IPv4 over L2 spine leaf topology

Figure 2 *Grand clock source connected to boundary clock (spines), followed by transparent clock leaves*
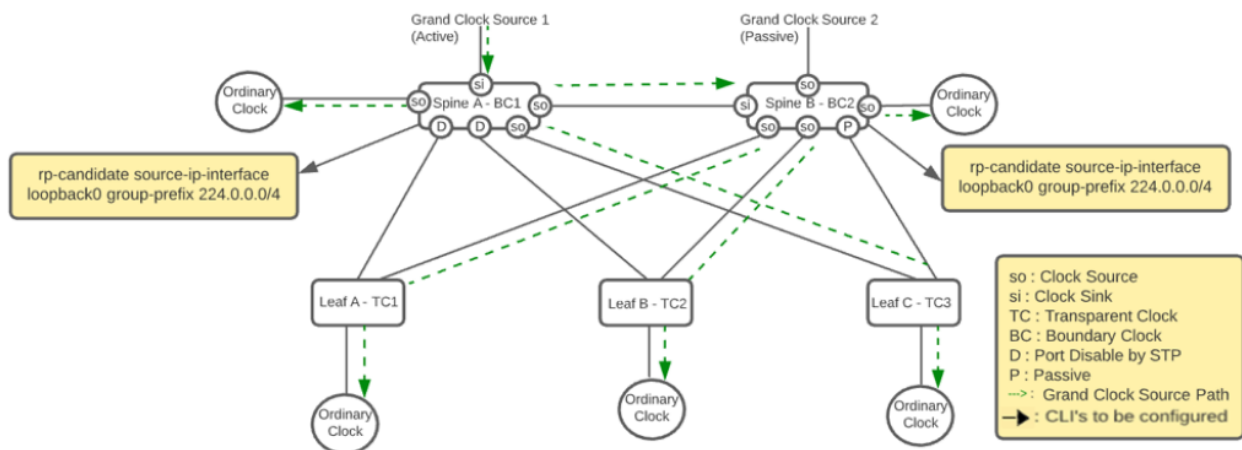
The following considerations and best practices apply to this use case illustrated in the above topology:

- Configure candidate-RP on switches that are connected to a grand clock source. The candidate-RP needs to be configured on the BC1 Spine A and BC2 Spine B.
- When the PTP clients are not capable of sending IGMP joins, be sure to configure `ip igmp-snooping static-group 224.0.1.129` on the VLAN interface of a TC, where PTP is configured.

In this case, it is an L2 switch in leaf so `ip igmp snooping enable` also needs to be configured on the transparent clock VLAN interface.

- Ensure that `ip source-interface ptp` is configured on both BC switches on the VLAN interface where PTP is configured.
- Ensure that `spanning tree` is enabled (the default) to avoid unwanted loops.
- In this use case topology, It is recommended to have VRRP on boundary clock switches to have L3 redundancy for PTP end clients.

Use case: PTP – L3 spine leaf topology

Figure 3 *Grand clock source connected to transparent clock, followed by boundary clock spines and boundary clock leaves*
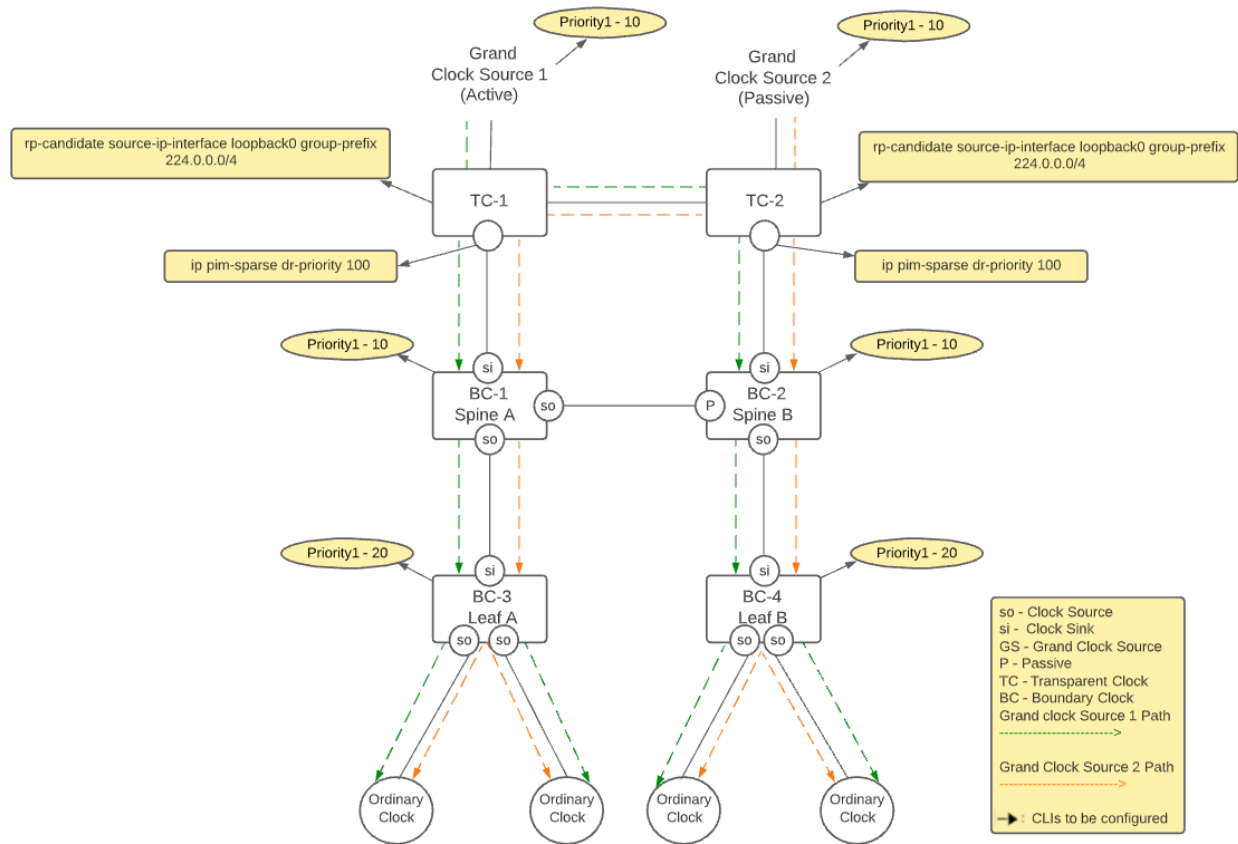
The following considerations and best practices apply to this use case illustrated in the above topology:

- Configure candidate-RP on switches which are connected to a grand clock source. Candidate-RP needs to be configured on TC1 and TC2. Each candidate-RP controls multicast traffic forwarding for one or more multicast groups.
- Configure higher DR priority on switches in which candidate-RP is configured. The DR priority needs to be configured on the TC1 and TC2 on the BC facing ports.
- When the PTP clients are not capable of sending IGMP joins, ensure that `ip igmp static-group 224.0.1.129` is configured on all PTP-enabled interfaces of a TC.
- The `igmp static-group` configuration is not needed on BC switches. In this case, it is an L3 network so `ip igmp enable` also needs to be configured on all PTP-enabled L3 interfaces of the TC.

Use case: PTP – BC and TC (VSF) topology connected via LAG

Figure 4 *Grand clock source connected to a boundary clock serving time to other boundary clocks and VSF transparent clocks in the network*
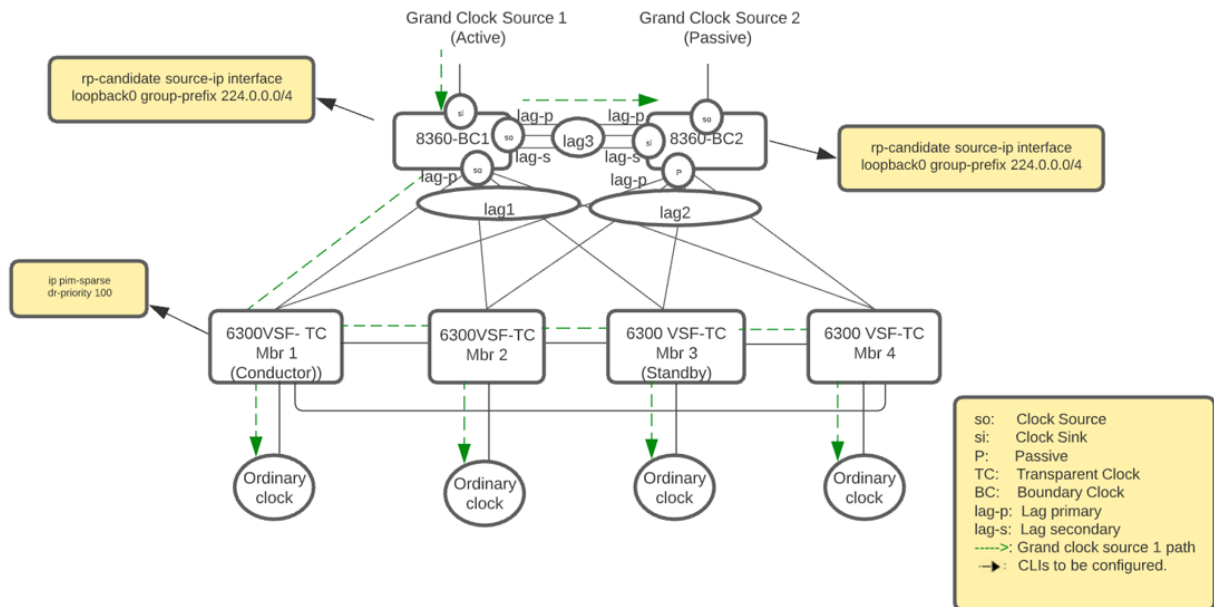
The following considerations and best practices apply to this use case illustrated in the above topology:

- Configure candidate-RP on switches that are connected to a grand clock source. The Candidate-RP needs to be configured on the BC1 and BC2 switches. Each candidate-RP controls multicast traffic forwarding for one or more multicast groups.

- When the PTP clients are not capable of sending IGMP joins, ensure that `ip igmp static-group 224.0.1.129` is configured on all PTP-enabled interfaces of a TC.

> `igmp static-group` config is not needed on boundary clock switches. In this case, it is an L3 network so `ip igmp enable` also needs to be configured on all PTP enabled L3 interfaces of the transparent clock.

- For the primary or secondary LAG roles, ensure that the same link ports are configured on both ends of the LAG across BC (this command is applicable only on BC switches).

> When both the primary and secondary LAG role links are down, PTP packets will not be forwarded even if other LAG links are up.

- Configure `ip pim-sparse dr-priority <PRIORITY-VALUE>` to configure higher dr-priority on the links originating from the VSF (which are facing the BC switches).

PTP commands

clear ptp statistics

```
clear ptp statisctics [<IFNAME>]
```

Description

Clears PTP counters for the given interface.

Parameter	Description
<IFNAME>	Optional: Specifies the interface name.

Examples

Clearing PTP counters for the given interface:

```
switch# clear ptp statistics 1/1/8
switch# clear ptp statistics lag1
switch# clear ptp statistics
```

Command History

Release	Modification
10.10.1000	Added boundary clock support on the 6300 Switch Series.
10.10	Command introduced on the 6300 Switch Series for transparent clock.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Administrators or local user group members with execution rights for this command.

clock-domain

```
clock-domain <DOMAIN-NUMBER>
no clock-domain
```

Description

Configures the PTP clock domain to a specified value.

The `no` form of this command removes the PTP domain configuration of the PTP clock.

Parameter	Description
<DOMAIN-NUMBER>	Sets the PTP clock domain. Range: 0 to 254. Value configurable subject to limits established by the PTP profile.

Usage

- The one-step end-to-end transparent clock works across domains.
- For boundary clocks, the clock-domain has to be identical with the domain used in the network.
- All PTP devices must be within same domain to be able to sync with each other.
- This command is only enabled in the PTP profile context.

Examples

Entering the PTP profile context and setting the PTP clock domain value:

```
switch(config)# ptp profile aes-r16
switch(config-ptp)#
switch(config-ptp)#clock-domain 4
switch(config-ptp)#
```

Removing the PTP clock domain value:

```
switch(config-ptp)# no clock-domain
switch(config-ptp)#
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	config-ptp	Administrators or local user group members with execution rights for this command.

clock-step

```
clock-step {one-step}
no clock-step
```

Description

Configures the clock step mode that determines when the egress-time information is sent.

The no form of this command removes the PTP clock-step configuration of the PTP clock.

Parameter	Description
one-step	Sets the PTP clock-step mode to one-step messaging in which egress-time information is sent along with the SYNC message.

Usage

- Mandatory command to start the PTP clock.

Example

Setting the clock-step mode to one-step messaging:

```
switch(config-ptp)# clock-step one-step
```

Removing the clock-step mode configuration:

```
switch(config-ptp)# no clock-step
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	config-ptp	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables the PTP profile globally. However, the PTP clock is started only when all the mandatory commands are set.

The `no` form of this command disables the PTP profile globally.

Usage

Mandatory command to start the PTP clock.

Examples

Enabling the PTP profile:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# enable
```

Disabling the PTP profile:

```
switch(config)# ptp profile 1588v2
```

```
switch(config-ptp)# no enable
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	`config-ptp`	Administrators or local user group members with execution rights for this command.

ip source-interface

```
ip source-interface {ptp | all} interface <IFNAME> [vrf <VRF-NAME>
ip source-interface {ptp | all} <IPV4-ADDR> [vrf <VRF-NAME>]
no ip source-interface {ptp | all} interface <IFNAME> [vrf <VRF-NAME>
no ip source-interface {ptp | all} <IPV4-ADDR> [vrf <VRF-NAME>]
```

Description

Configures the source IP address to be used when sending PTP messages. Use the `ptp` keyword to set source IP address specific to the PTP feature. If the feature-specific configuration is not available, the source IP address corresponding to the `all` option will be used.

The `no` form of this command removes the configuration of the source IP address used by the PTP feature.

Parameter	Description
`ptp`	Selects the PTP protocol.
`all`	Selects all protocols that can be configured by this command.
`interface <IF-NAME>`	Specifies the name of the interface from which the source IP address is obtained. The interface must have a valid IP address assigned to it. If the interface has both a primary and secondary IP address, the primary IP address is used.
`vrf <VRF-NAME>`	Specifies the VRF name.
`<IPV4-ADDR>`	Specifies the source IPv4 address to be used. The IP address must be defined on the switch, and it must exist on the specified VRF (which is the default VRF, if the vrf option is not used). Specify the address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.

Usage

- This command must be configured on the switch when PTP is enabled on VLAN trunk or access ports, and the transport protocol is IPv4.

- In the current version of PTP, only the default VRF is supported.
- This command is not applicable to the end-to-end transparent clock.

Examples

Configuring the source IP address for sending PTP messages:

```
switch(config)# ip source-interface ptp interface 1/1/1
switch(config)# ip source-interface ptp 10.10.10.1
switch(config)# ip source-interface ptp interface vlan10
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	`config`	Administrators or local user group members with execution rights for this command.

mode

```
mode boundary end-to-end
no mode boundary end-to-end
mode transparent end-to-end
no mode transparent end-to-end
```

Description

Configures the switch PTP clock mode, either boundary or transparent, with a delay-request mechanism of end-to-end. A device in transparent clock mode does not synchronize (syntonize) itself to a grandsource clock.

Boundary clock is available on the 6300 Switch Series models R8S89A and, R8S90A.

The `no` form of this command unconfigures the PTP clock mode.

Parameter	Description
`boundary`	Selects boundary clock mode.
`transparent`	Selects transparent clock mode.
`end-to-end`	Selects the end-to-end delay-request mechanism.

Examples

Configuring PTP boundary end-to-end clock mode:

```
switch(config-ptp)# mode boundary end-to-end
```

Unconfiguring PTP boundary end-to-end clock mode:

```
switch(config-ptp)# no mode boundary end-to-end
```

Configuring PTP transparent end-to-end clock mode:

```
switch(config-ptp)# mode transparent end-to-end
```

Unconfiguring PTP transparent end-to-end clock mode:

```
switch(config-ptp)# no mode transparent end-to-end
```

Command History

Release	Modification
10.10.1000	Added boundary clock to the 6300 Switch Series models R8S89A and, R8S90A.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	`config-ptp`	Administrators or local user group members with execution rights for this command.

priority1

```
priority1 <PRIORITY>
no priority1
```

Description

Configures the PTP clock `priority1` value of the device. This value is operational when the device is in boundary clock mode and participating in the Best Clock Source Algorithm (BMCA). This value is used to indicate priority to its downstream clock-aware devices.

The `no` form of this command removes the PTP `priority1` configuration of the PTP clock and sets it to the default value of 128.

Parameter	Description
`<PRIORITY>`	Sets the priority value. Default 128.

Usage

This value can be configured only for the boundary clock.

Examples

Configuring PTP priority1 value:

```
switch(config-ptp)# priority1 129
```

Removing PTP priority1 configuration:

```
switch(config-ptp)# no priority1
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	config-ptp	Administrators or local user group members with execution rights for this command.

priority2

```
priority2 <PRIORITY>
no priority2 <PRIORITY>
```

Description

Configures the PTP clock `priority2` value of the device. This value is operational when the device is in boundary clock mode and participating in the Best Clock Source Algorithm (BMCA). This value is used to indicate priority to its downstream clock-aware devices.

The `no` form of this command removes the PTP `priority2` configuration of the PTP clock and sets it to the default value of 128.

Parameter	Description
<PRIORITY>	Sets the priority value. Default 128.

Usage

This value can be configured only for the boundary clock.

Examples

Configuring PTP `priority1` value:

```
switch(config-ptp)# priority2 129
```

Removing PTP priority2 configuration:

```
switch(config-ptp)# no priority2
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-ptp`	Administrators or local user group members with execution rights for this command.

ptp announce-interval

```
ptp announce-interval {1588v2| aes67 | aes-r16 | smpte} <LOG-SECONDS>
no ptp announce-interval {1588v2| aes67 | aes-r16 | smpte}
```

Description

Sets the announce message transmit interval on a PTP-enabled interface for a specific PTP profile.

The `no` form of this command removes the announce message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Default: 1.
`aes67`	Specifies the PTP AES67 profile timers. Default: 1.
`aes-r16`	Specifies the PTP AES-R16 profile timers. Default: 1.
`smpte`	Specifies the PTP SMTPE profile timers. Default: -2.
`<LOG-SECONDS>`	Sets the announce message interval in log seconds.

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP AES67 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-interval aes67 2
```

Removing the PTP AES67 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp announce-interval aes67
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-if`	Administrators or local user group members with execution rights for this command.

ptp announce-timeout

```
ptp announce-timeout {1588v2| aes67 | aes-r16 | smpte} <COUNT>
no ptp announce-timeout {1588v2| aes67 | aes-r16 | smpte}
```

Description

Sets the announce message receipt timeout on a PTP-enabled interface for a specific PTP profile.

The `no` form of this command resets the announce message receipt timeout configuration on a PTP-enabled interface and sets a profile-specific default value.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Default: 3.
`aes67`	Specifies the PTP AES67 profile timers. Default: 3.
`aes-r16`	Specifies the PTP AES-R16 profile timers. Default: 3.
`smpte`	Specifies the PTP SMTPE profile timers. Default: 3.
`<LOG-SECONDS>`	Specifies the number of announcement intervals.

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP AES67 profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp announce-timeout aes67 4
```

Resetting the PTP AES67 profile timer:

```
switch(config)# interface 1/1/1
switch(config-if)#no ptp announce-timeout aes67
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-if`	Administrators or local user group members with execution rights for this command.

ptp clock-source-only

```
ptp clock-source-only
no ptp clock-source-only
```

Description

Configures the PTP port state to clock_source state. This prohibits the port from entering into a clock_sink or passive state.
The no form of this command removes the clock_source state configuration on the port and returns it to normal BMCA operation.

Usage

This can only be configured for the boundary clock.

Examples

Configuring the clock_source only role for the port:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp clock-source-only
```

Removing the configuration of clock_source only role for the port:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp clock-source-only
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-if`	Administrators or local user group members with execution rights for this command.

ptp delay-req-interval

```
ptp delay-req-interval {1588v2 | aes67 | aes-r16 | smpte} <LOG-SECONDS>
no ptp delay-req-interval {1588v2 | aes67 | aes-r16 | smpte}
```

Description

Sets the `delay_req` message transmit interval on a PTP-enabled interface for a specific PTP profile.

The `no` form of this command removes the `delay_req` message transmit interval configuration on a PTP-enabled interface and sets a profile specific default value.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Default 0.
`aes67`	Specifies the PTP AES67 profile timers. Default 0.
`aes-r16`	Specifies the PTP AES-R16 profile timers. Default 0.
`smpte`	Specifies the PTP SMTPE profile timers. Default -3.
`<LOG-SECONDS>`	Sets the `delay_req` message interval in log seconds.

Usage

This value can be configured only for the boundary clock.

Examples

Setting the PTP AES67 profile timers:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp delay-req-interval aes67 2
```

Removing the PTP AES67 profile timer configuration:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp delay-req-interval aes67
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-if`	Administrators or local user group members with execution rights for this command.

ptp enable

```
ptp enable
no ptp enable
```

Description

Enables PTP on the interface. The `no` form of this command disables PTP on the interface.

Examples

Enabling PTP on a physical interface:

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

Disabling PTP on the interface context:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp enable
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	`config-if`	Administrators or local user group members with execution rights for this command.

ptp lag-role

```
ptp lag-role {primary | secondary}
no ptp lag-role
```

Description

Configures the PTP role for the member interfaces of a Link Aggregation (LAG) . When there are two or more member interfaces for a LAG, only one link can be configured as primary and only one other link can be configured as secondary. The primary member interface is used for transmitting the PTP packets generated by the boundary clock. When the primary member goes down, the secondary member is used for PTP packet transmission. If both primary and secondary members go down, PTP does not flip over to the other links of the LAG.

The `no` form of this command removes the PTP role configuration for the LAG member interface.

This command is not supported when configured as a transparent clock.

Parameter	Description
primary	Sets the primary PTP lag-role for the LAG member interface.
secondary	Sets the secondary PTP lag-role for the LAG member interface.

Usage

- LAG roles must be configured for boundary clock.
- For the primary or secondary LAG roles, ensure that the same link ports are configured on both ends of the LAG.

Examples

Setting the primary PTP lag-role for the LAG member interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp lag-role primary
```

Setting the secondary PTP lag-role for the LAG member interface:

```
switch(config)# interface 1/1/2
switch(config-if)# ptp lag-role secondary
```

Removing the PTP lag-role configuration for the LAG member interface:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp lag-role
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	config-if	Administrators or local user group members with execution rights for this command.

ptp peer ip

```
ptp peer ip <IP-ADDRESS>
no ptp peer ip <IP-ADDRESS>
```

Description

Configures destination IP addresses for the interfaces in unicast transmission. The `no` form of this command removes the PTP destination IP address configuration for the interfaces in unicast transmission.

Parameter	Description
ip <IP-ADDRESS>	Specifies the peer IPv4 address. Syntax: A.B.C.D

Usage

This command has no effect when configured as a transparent clock.

Example

Configuring `ptp peer ip` on the interface:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp peer ip 10.0.0.1
```

Removing `ptp peer ip` on the interface:

```
switch(config-if)# no ptp peer ip 10.0.0.1
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	config-if	Administrators or local user group members with execution rights for this command.

ptp profile

```
ptp profile {<PROFILE NAME>}
no PTP profile
```

Description

Enters the PTP context to configure the PTP profile in which the device will operate.

Configure PTP profile before configuring mode or other profile-specific parameters. The device can be operating in any one profile at a given point of time. The `no` form of this command removes the PTP profile configuration in which the device will operate. This command clears the PTP profile and all parameters related to that profile.

Parameter	Description
<PROFILE NAME>	Specifies the profile to be used. Profiles include: ■ 1588v2: Specifies the IEEE 1588-2008 profile to be used. ■ aes-r16: Specifies the IEEE AES-R16-2016 profile to be used. ■ aes67: Specifies the IEEE AES67 profile to be used. ■ smpte: Specifies the IEEE SMPTE-ST-2059-2 profile to be used.

Usage

Configure PTP profile before configuring mode or other profile-specific parameters.

Example

Configuring PTP profiles:

```
switch(config)# ptp profile 1588v2
```

Configuring more than one PTP profile:

```
switch(config)# ptp profile 1588v2
switch(config-ptp)# exit
switch(config)# ptp profile smpte
switch(config-ptp)#
The existing profile must be removed using the 'no ptp profile' command before
configuring a different profile.
```

Removing the PTP profile:

```
switch(config-ptp)# no ptp profile
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	`config`	Administrators or local user group members with execution rights for this command.

ptp sync-interval

```
ptp sync-interval {1588v2| aes67 | smpte} <LOG-SECONDS>
no ptp sync-interval {1588v2 | aes67 | smpte}
```

Description

Sets the sync message transmit interval on a PTP-enabled interface for a specific PTP profile.

The `no` form of this command removes the sync message transmit interval configuration on a PTP enabled interface and sets it to a profile-specific default value.

Parameter	Description
`1588v2`	Specifies the PTP 1588v2 profile timers. Default 0.
`aes67`	Specifies the PTP AES67 profile timers. Default -3.
`smpte`	Specifies the PTP SMTPE profile timers. Default -3
`<LOG-SECONDS>`	Sets the sync message interval in log seconds.

Examples

Setting the PTP 1588v2 sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval 1588v2 2
```

Setting the PTP AES67 sync interval :

```
switch(config)# interface 1/1/1
switch(config-if)# ptp sync-interval aes67 -2
```

Removing the PTP AES67 sync interval:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp sync-interval aes67
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-if`	Administrators or local user group members with execution rights for this command.

ptp vlan

```
ptp vlan <VLAN-ID>
no ptp vlan
```

Description

Configures a VLAN for PTP messages. It is necessary when the boundary clock port is a VLAN trunk L2 interface (`no routing`). The `no` form of this command removes the VLAN configuration for PTP messages.

Parameter	Description
`<VLAN-ID>`	Specifies a VLAN. Range: 1-4094.

Usage

- This configuration has no bearing on the one-step transparent clock.
- In boundary clock mode, only PTP packets in PTP VLAN are processed; PTP packets from other VLANs are dropped.
- `ptp vlan` should be configured on interfaces only when the specific VLAN is a trunk/tagged member of that port. This configuration should not be performed on an access port.

Examples

Configuring a specific VLAN for PTP messages:

```
switch(config)# interface 1/1/1
switch(config-if)# ptp vlan 4
```

Removing the VLAN configuration for PTP messages:

```
switch(config)# interface 1/1/1
switch(config-if)# no ptp vlan
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	`config-if`	Administrators or local user group members with execution rights for this command.

show ptp clock

```
show ptp clock
```

Description

Shows PTP clock-related information.

Example

Showing PTP transparent clock information:

```
switch# show ptp clock
PTP Profile                      : smpte
PTP Mode                         : transparent
Delay Mechanism                  : end-to-end
Clock Identity                   : NA
Network Transport Protocol       : ipv4
Clock Step                       : One
Clock Domain                     : NA
Number of PTP Ports              : 1
Priority1                        : NA
Priority2                        : NA
Clock Quality :
  Class                          : NA
  Accuracy                       : NA
  Offset (log variance)          : NA
Offset From Clock-Source         : NA
Mean Delay                       : NA
Steps Removed                    : NA
```

Showing PTP boundary clock information (boundary clock is available only on the 6300 Switch Series models R8S89A and R8S90A that first released with AOS-CX 10.10.1000):

```
switch# show ptp clock
PTP Profile                      : aes67
PTP Mode                         : boundary
Delay Mechanism                  : end-to-end
Clock Identity                   : 00:fd:45:ff:fe:68:f3:00
Network Transport Protocol       : ipv4
Clock Step                       : Two
Clock Domain                     : 0
Number of PTP Ports              : 3
Priority1                        : 128
Priority2                        : 128

Clock Quality :
  Class                          : 248
  Accuracy                       : 49
  Offset (log variance)          : 52592
```

```
Offset From Clock-Source           : - 0.000000006  (s)
Mean Delay                         : + 0.000000277  (s)
Steps Removed                      : 1
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp foreign-clock-sources

```
show ptp foreign-clock-sources
```

Description

Shows the priority1, priority2, class, accuracy, offset-scaled-log-variance (OSLV), and steps removed information for foreign clock-source nodes.

Example

Showing PTP foreign clock-source information:

```
switch(config-if)# show ptp foreign-clock-sources
P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-scaled-log-variance, SR=Steps-removed


---------- ----------------------------- ----------------------- ---- ---- ---- ---- ------ ---
Interface  Foreign Port ID                Clock Source ID          P1   P2   C    A    OSLV   SR
---------- ----------------------------- ----------------------- ---- ---- ---- ---- ------ ---
1/1/4      00:00:00:00:00:00:00:01(0x0001) 00:00:00:00:00:00:00:01  0    0    6    35   0      1
1/1/5      b4:99:ba:ff:fe:54:2b:00(0x0002) 00:00:00:00:00:00:00:01  0    0    6    35   0      2
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp interface

```
show ptp interface [<IFNAME> | [brief]
```

Description

Shows PTP port-related information.

Parameter	Description
<IFNAME>	Specifies the interface name.
brief	Shows information in a brief format.

Examples

Showing PTP port information when the switch is acting as a transparent clock:

```
switch# show ptp interface 1/1/1
Port Identity                       : NA
Port Number                         : NA
PTP Version                         : 2
PTP Enable                          : Enabled
Transport of PTP                    : ipv4
Port State                          : Running
Delay Mechanism                     : end-to-end
Announce Interval (log mean)        : NA
Announce Receipt Timeout            : NA
Sync Interval (log mean)            : NA
Sync Timeout                        : NA
Delay Request Interval (log mean)   : NA
switch#

switch# show ptp interface lag20
Port Identity                       : NA
Port Number                         : NA
PTP Version                         : 2
PTP Enable                          : Enabled
Transport of PTP                    : ipv4
Port State                          : NA
Delay Mechanism                     : end-to-end
Announce Interval (log mean)        : NA
Announce Receipt Timeout            : NA
Sync Interval (log mean)            : NA
Sync Timeout                        : NA
Delay Request Interval (log mean)   : NA
switch#
```

Showing PTP port information when the switch is acting as a boundary clock (boundary clock is available only on the 6300 Switch Series models R8S89A and R8S90A that first released with AOS-CX 10.10.1000):

```
switch# show ptp interface 1/1/1
Interface : 1/1/1
Port Identity                         : 88:3a:30:ff:fe:05:c9:80 (port: 0x0002)
Port Number                           : 2
PTP Version                           : 2
PTP Enable                            : Enabled
Transport of PTP                      : ethernet
Port State                            : Clock Source
Delay Mechanism                       : end-to-end
Announce Interval (log mean)          : 0
Announce Receipt Timeout              : 3
Sync Interval (log mean)              : -3
Sync Timeout                          : NA
Delay Request Interval (log mean)     : 0

switch# show ptp interface lag1
Port Identity                         : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                           : 2
PTP Version                           : 2
PTP Enable                            : Enabled
Transport of PTP                      : ipv4
Port State                            : Clock Source
Delay Mechanism                       : end-to-end
Announce Interval (log mean)          : 0
Announce Receipt Timeout              : 3
Sync Interval (log mean)              : -3
Sync Timeout                          : NA
Delay Request Interval (log mean)     : -3
Primary Interface                     : 1/1/5
Secondary Interface                   : 1/1/6

switch# show ptp interface
Interface lag20:
Port Identity                         : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                           : 2
PTP Version                           : 2
PTP Enable                            : Enabled
Transport of PTP                      : ipv4
Port State                            : Clock Source
Delay Mechanism                       : end-to-end
Announce Interval (log mean)          : 0
Announce Receipt Timeout              : 3
Sync Interval (log mean)              : -3
Sync Timeout                          : NA
Delay Request Interval (log mean)     : -3
Primary Interface                     : 1/1/5
Secondary Interface                   : 1/1/6

Member Interface 1/1/5:
Port Identity                         : 00:fd:45:ff:fe:68:f3:00 (port: 0x0002)
Port Number                           : 2
PTP Version                           : 2
PTP Enable                            : Enabled
Transport of PTP                      : ipv4
Port State                            : Running
Delay Mechanism                       : end-to-end
Announce Interval (log mean)          : 0
Announce Receipt Timeout              : 3
Sync Interval (log mean)              : -3
Sync Timeout                          : NA
Delay Request Interval (log mean)     : -3
```

```
Member Interface 1/1/6:
Port Identity                       : 00:fd:45:ff:fe:68:f3:00 (port: 0x0003)
Port Number                         : 3
PTP Version                         : 2
PTP Enable                          : Enabled
Transport of PTP                    : ipv4
Port State                          : Not Running
Delay Mechanism                     : end-to-end
Announce Interval (log mean)        : 0
Announce Receipt Timeout            : 3
Sync Interval (log mean)            : -3
Sync Timeout                        : NA
Delay Request Interval (log mean)   : -3

Interface 1/1/15:
Port Identity                       : 00:fd:45:ff:fe:68:f3:00 (port: 0x0001)
Port Number                         : 1
PTP Version                         : 2
PTP Enable                          : Enabled
Transport of PTP                    : ipv4
Port State                          : Clock Sink
Delay Mechanism                     : end-to-end
Announce Interval (log mean)        : 0
Announce Receipt Timeout            : 3
Sync Interval (log mean)            : -3
Sync Timeout                        : NA
Delay Request Interval (log mean)   : -3
```

Showing PTP port information (in brief form) when the switch is acting as a boundary clock (boundary clock is available only on the 6300 Switch Series models R8S89A and R8S90A that first released with AOS-CX 10.10.1000):

```
switch# show ptp interface brief
Interface       PTP State
------------------------
1/1/11          Clock Sink
1/1/12          Clock Source
1/1/15          Clock Source
1/1/16          Clock Source
```

Showing PTP port information in brief format:

```
switch# show ptp interface brief
Interface  PTP State
------------------------
1/1/1      Running
1/1/2      Running
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp parent

```
show ptp parent
```

Description

Shows parent node information for the PTP device.

Example

Showing PTP parent node information:

```
switch# show ptp parent
PTP Parent Properties

Parent Clock
---------------------------
Parent Clock Identity               : 00:00:00:00:00:00:00:01
Parent Port Number                  :  0x0001
Observed Parent Offset (log variance)  : 65535
Observed Parent Clock Phase Change Rate: 2147483647

Grandsource Clock
---------------------------
Grandsource Clock Identity          : 00:00:00:00:00:00:00:01
Grandsource Clock Quality
  Class                             : 6
  Accuracy                          : 35
  Offset (log variance)             : 0
Priority1                           : 0
Priority2                           : 0
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show ptp statistics

```
show ptp statistics [<IFNAME>]
```

Description

Shows PTP port statistics.

Parameter	Description
<IFNAME>	Optional. Specifies the interface name.

Examples

Showing PTP port statistics:

```
switch# show ptp statistics

PTP Interface Statistics

              Received Packets    Sent Packets   Discarded Packets   Lost Packets
Interface: 1/1/15
    Announce                 0            1019                   0              0
    Sync                     0            2038                   0              0
    Signaling                0               0                   0              0
    DelayReq                 0               0                   0              0
    DelayResp                0               0                   0              0
    FollowUp                 0               0                   0              0
    Management               0               0                   0              0

              Received Packets    Sent Packets   Discarded Packets   Lost Packets
Interface: 1/1/16
    Announce                 0            1019                   0              0
    Sync                     0            2038                   0              0
    Signaling                0               0                   0              0
    DelayReq                 0               0                   0              0
    DelayResp                0               0                   0              0
    FollowUp                 0               0                   0              0
    Management               0               0                   0              0
```

Showing PTP port statistics for the specified interface:

```
switch# show ptp statistics 1/1/15

PTP Interface Statistics

              Received Packets    Sent Packets   Discarded Packets   Lost Packets
Interface: 1/1/15
    Announce                 0            1024                   0              0
    Sync                     0            2048                   0              0
    Signaling                0               0                   0              0
    DelayReq                 0               0                   0              0
    DelayResp                0               0                   0              0
    FollowUp                 0               0                   0              0
    Management               0               0                   0              0
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Administrators or local user group members with execution rights for this command.

show ptp time-property

```
show ptp time-property
```

Description

Shows PTP clock-time properties for the PTP device.

Example

Showing PTP clock time properties:

```
switch # show ptp time-property
PTP Clock Time Property
---------------------------
Current UTC Offset Valid  : FALSE
Current UTC Offset        : 37
Leap59                    : FALSE
Leap61                    : FALSE
Time Traceable            : FALSE
Frequency Traceable       : FALSE
PTP Timescale             : FALSE
Synchronization Uncertain : FALSE
Time Source               : 160
```

Command History

Release	Modification
10.10.1000	Command introduced on the 6300 Switch Series.
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300 (only R8S89A, R8S90A)	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

show running-config ptp

```
show running-config ptp
```

Description

Shows PTP running configuration related information.

Example

Showing PTP running configuration information (boundary clock is available only on the 6300 Switch Series models R8S89A and R8S90A that first released with AOS-CX 10.10.1000):

```
switch# show running-config ptp
Current configuration:
ptp profile smpte
        enable
        clock-step one-step
        transport-protocol ipv4
        mode boundary end-to-end
interface 1/1/1
        no shutdown
        ip address 50.1.1.0/31
        ptp enable
        ptp clock-source-only
```

Command History

Release	Modification
10.08 or later	Command introduced.

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

transport-protocol

```
transport-protocol {ethernet | ipv4}
no transport-protocol
```

Description

Sets the transport protocol for PTP packets. In the case of IPv4, the UDP check-sum is reset. There is no default transport-protocol. The `no` form of this command disconnects the clock from its source.

Parameter	Description
ethernet	Specifies the Ethernet (Layer 2) transport protocol.
ipv4	Specifies the IPv4 transport protocol.

Usage

Mandatory command to start the PTP clock.

Example

Setting the Ethernet transport protocol for PTP packets:

```
switch(config-ptp)# transport-protocol ethernet
```

Removing the transport protocol for PTP packets:

```
switch(config-ptp)# no transport-protocol
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
6300	config-ptp	Administrators or local user group members with execution rights for this command.

Upgrade and downgrade scenarios

Upgrade and downgrade scenarios are provided by the Configuration Migration Framework (CMF).

Upgrades

All upgrade scenarios are supported and configuration is migrated.

Downgrades

The following scenario is supported:

1. Create a checkpoint before upgrading.
2. Upgrade.
3. Perform config changes.
4. Set the startup configuration to the checkpoint created in step 1.
5. 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

In service software upgrade

In-Service Software Upgrade (ISSU) is the name given to a mechanism used to upgrade a device without affecting the service it is providing. In the case of switches, this means that the traffic won't be interrupted during the upgrade and if an error happens and traffic is interrupted to keep the interruption as short as possible.

Aruba's switch architecture decouples the control plane and the data plane, so it is possible to implement an ISSU mechanism by keeping the data plane up while the control plane manages the upgrade.

ISSU is supported for upgrades between minor releases.

This document describes the design and considerations for ISSU for the Aruba 6400 Switch Series. It does not cover ISSU for other Aruba Switch Series or for VSF.

Problem description

The main problem ISSU solves is the need to reboot the switch when doing an upgrade. Before ISSU is implemented, the only supported way of upgrading is through a reboot. ISSU allows this upgrade operation to happen without interrupting traffic, even when there is a reboot of the management modules and an upgrade of line card modules.

Use cases

ISSU is designed to upgrade the current device's firmware without interrupting traffic. This attribute is critical in some scenarios where a network outage would mean a very disruptive event. The following are examples of such scenarios:

- **Health care networks:** In this scenario, the medical devices connected to the switch must not stop sending information to monitoring stations. These devices could be connected to the switch directly or through a wireless access point. In this case, the access points must not be interrupted.

- **IoT networks:** Many small devices depend on network traffic to remain connected to a central command center. If traffic is interrupted, these IoT devices could lose the connection to the central place and stop sending critical data.

Upgrade scope

The current ISSU feature is aimed to do upgrades between major and minor releases. This is suitable for stable networks that need critical bug fixes or security fixes instead of full version upgrades to get new functionality.

Operation

ISSU in the 6400 consists in a set of steps designed to keep the system in a stable state while the firmware is upgraded and to recover this state after such upgrade.

Step 1: Image download and validation

The first step of the process is to download the image with the new version of the firmware and verify it complies with the ISSU rules and the security checks (e.g., valid signed image). These rules are internal checks which verify that the ISSU operation can be performed between the current image running in the switch and the new one.

Upon successful verification the new image will be installed in the bank that doesn't store the image currently running on the switch. The old image will be kept in the alternative bank in case a fail back process needs to be triggered due to an error.

Step 2: Install the image in the standby management module

Once the new image is verified, the Standby Management Module (SMM) will be upgraded with this image. Note that during this process there is no redundancy between MMs and any fatal error in the Active Management Module (AMM) will mean a switch reboot (more on this in the Errors and Recovery section).

Step 3: Freeze the system

Once the SMM is successfully upgraded, the system's state will be frozen. This means that no further configuration will be allowed until ISSU is complete. In fact, no configuration via CLI, REST, or SNMP is allowed once the ISSU process starts (Step 1) to make sure the system doesn't become unstable once ISSU has started. Informational queries are still allowed. Any change in the network will not be reflected until ISSU is complete. E.g., MAC learning. Please refer to Information not updated during ISSU for additional information.

Step 4: Perform the upgrade for the line card modules

The Line Card (LC) modules will be upgraded at this time, however they will not be rebooted.

Step 5: Recover the previous state

The previous state will be recovered and synchronized with the new firmware running in the SMM. Some features can't recover the previous state at this point and therefore do not support uninterrupted operation during ISSU. Please refer to Features that don't support uninterrupted operation during ISSU for more information.

Step 6: Failover occurs between the AMM and the SMM

The SMM will take the Active Management Module role using the new firmware version. All sessions will be closed and the user will be required to login again.

Step 7: The previous AMM will upgrade its image

The previous AMM will upgrade its image and take the role of Standby Management Module. The ISSU is complete at this point.

Considerations

The first requirement for ISSU is to ensure traffic continues to pass through the switch uninterrupted during the upgrade operation. If something goes wrong, traffic must be restored as soon as possible. This could mean falling back to the previous image, or in some cases to fall forward to the new one.

The upgrade process can take minutes to complete. During that time as many control plane protocols as possible will remain operational, however some of them need to stop processing packets or avoid reacting to events. Please refer to Information not updated during ISSU for additional information. The amount of time where they are not operational will be kept as small as possible. The only full control plane disruption is similar to the disruption caused by an HA failover event. This means that ISSU will be as hitless as an HA failover. If a feature is not hitless during an HA failover then it won't be hitless during ISSU. Please refer to Features that don't support uninterrupted operation during ISSU for additional information.

In order to start ISSU, all modules (i.e., LCs, fabric cards, management modules) must be operational and running. If any of them is in another state (e.g., failover, line cards not ready, etc.) the ISSU process will not start.

Limitations

The ISSU process currently has the following limitations and considerations:

Management modules

In order for ISSU to work the switch chassis needs to have two management modules installed.

Line card support

The ISSU version released in 10.10 only supports line cards with model numbers ending in A or B, i.e. LCs with model numbers following the format "ROX_A" and "ROX_B". Newer LCs will be supported in later versions. Mixed mode (i.e. a chassis with A or B line cards and newer line cards) is not supported in ISSU.

Hardware faults

It is recommended that hardware faults are resolved prior to performing ISSU. Fan faults and abnormal temperature statuses should be addressed. Fans may increase in speed during the ISSU process.

Prohibited operations

During ISSU the following operations are not permitted:

- Any hardware hot swap
- Pressing any button

Performing any of these operations during an ISSU could put the system in an error state that could adversely affect the ISSU.

The system may not be able to address failures during the ISSU. E.g., if network protocols require blocking a port, flush MAC, or routing tables, etc. the switch would not be able to react to those tasks until the ISSU is complete.

Scheduled jobs

Since no configuration is allowed during the ISSU, it is possible that some scheduled jobs will fail if they are attempted while the ISSU is in progress. Users can check for the "`ISSU is in-progress, configuration`

`is not allowed`" message to find out if any scheduled job has failed. It is recommended to not execute any scheduled job during ISSU.

Information not updated during ISSU

During ISSU the following information may not be current until after ISSU completes:

- Link state. Transitions may not be reflected until ISSU is done.
- Temperatures.
- Power consumption values.
- System state as indicated by LEDs.
- MAC Learning.
- Change in MAC for a neighbor via Gratuitous ARP.
- Some counters will stop increasing their value during ISSU.

Show tech

The show tech command is enabled during ISSU using the CLI, however it isn't possible to use it with the REST API.

Features that don't support uninterrupted operation during ISSU

During ISSU the following features may be interrupted until after ISSU completes:

PIM with MSDP

Currently, PIM is not supported in ISSU on RP routers, therefore traffic loss is expected during ISSU on RP routers where PIM and MSDP are enabled.

Dynautz ISSU

All Dynamic Authorization requests will be rejected with NAK during ISSU operation.

BFD ISSU

It's important to note that this mechanism is only recommended for sessions that have a failure detection time higher than 6 seconds (e.g. Tx=Rx=3000 and Detect Multiplier=2, or Tx=Rx=2000 and Detect Multiplier=3). The setup should have less than 64 sessions, otherwise the ISSU failover might not be hitless for all sessions.

NAE

NAE will have a momentary disruption during ISSU events due to the failover event. See the Network Analytics Engine Guide for more information.

Feature readiness check

ISSU will fail if the feature ready check does not pass. The feature ready check validates that none of the following features are in a failed state:

- ACLs, object groups, and their applications
- Classifier policies, classes, and their applications
- Port-access polices, classes, and their applications
- Port-access group-based policies, classes, and their applications
- Active PBR actions and their applications

In general, if any of the above is in a failed state Aruba recommends fixing it and then upgrading to the newer operating system image using the system reboot method instead of ISSU. Some of the failed state will remain even after it is fixed on a running system and a reboot is good best practice for clearing it.

There are system validation checks to ensure that all line card part numbers end in an A or B.

VSX environments

In order to minimize a potential downtime, it is strongly recommended that in a VSX topology ISSU is performed at different times for each switch. E.g.,

run ISSU on the primary switch, verify that it was successful, and then perform ISSU for the secondary switch.

Errors and recovery

During ISSU there are several different error recovery actions, depending on the ISSU step where the error occurs. The system may be able to recover from a single failure, but it is not possible to recover from a double failure. A double failure would require a full switch reboot.

There are two types of errors during ISSU: recoverable errors and unrecoverable errors.

Recoverable errors are handled by aborting the ISSU process and getting back to a stable system without impacting the data plane. Recoverable errors fall back to the current version.

Unrecoverable errors require either a LC reboot or an MM reboot depending on where the error occurs. If some conditions are met (e.g., double failure, MM-LC failure) it is possible that a full switch reboot is needed.

The following are scenarios that would mean an error during ISSU:

Firmware errors

- New version is not a valid target
- SMM fatal errors before the failover

SMM errors

- SMM doesn't boot correctly
- Critical process crash

LC upgrade errors

- An LC failing while executing any of the ISSU steps

Error handling definitions

Possible ways to handle an ISSU error:

Abort Hitless

- ISSU is aborted with no traffic interruption
- No traffic impact
- Recoverable
- Abort hitless before the SMM software upgrade means that ISSU is not started
- Abort hitless after the SMM software upgrade means that SMM reboots to current version
- No upgrade occurs

Abort with non-recoverable errors

- ISSU is aborted and traffic was interrupted
- Traffic Impact
- All affected LCs are moved to an error state
- Affected LCs and SMM rebooted to current version
- No upgrade occurs

Complete with non-recoverable errors

- Upgrade was done, but with errors
- Traffic impact
- All affected LCs are moved to an error state
- Affected LCs rebooted to new version after ISSU is completed
- Upgrade complete

Fail forward with non-recoverable errors

- ISSU operation fails and new image is used for recovery
- Traffic impact
- Chassis reboots to new version (AMM, SMM, LCs)
- Upgrade complete

Error Handling

Each step of the ISSU process has different ways to handle errors. Errors will be managed based on which stage of the ISSU process the system is currently on.

Image download and validation

If during .swi file validation the system finds out that the target image is not suitable for ISSU or that it is not compatible with the current version, the ISSU process will not be started. The error will be handled as abort hitless.

Install image in the SMM

If during the SMM software upgrade the new image fails to install or to boot to a valid state, then the ISSU process will be aborted. The error will be handled as abort hitless and the SMM reboots to current version.

System freeze

If the error happens while the system state is frozen, then the system needs to be thawed. This means taking it out of the frozen state and restoring the previous state without interrupting traffic. Any change done by the ISSU must be reverted. The ISSU process is aborted. The error will be handled as abort hitless. There are some cases where the system cannot be thawed. In this case the LCs will reboot to the new image since the system cannot recover the previous state. The error will be handled as fail forward.

Perform the upgrade for the line card modules

If any of the modules running in the LCs fail to upgrade, the line card will be marked as in an error state and it will wait until the ISSU process is done. The error will be handled as complete with errors.

Recover the previous state

Once the upgrade is complete, the system will start to recover the previous state. If there is an error recovering the line card's previous state, the line card will be marked as in an error state and it will wait until ISSU is over before coming back. The error will be handled as complete with errors.

If the previous state cannot be recovered for all LCs or for the whole system, a system reboot is required to reach a known state. The system will boot with the new image. The error will be handled as fail forward.

Failover

The last step in the ISSU process is to do a failover where the SMM becomes the AMM. If the failover fails, the whole chassis will be rebooted. The system will boot with the new image. The error will be handled as fail forward and the previous AMM will upgrade its image. After the failover, the ISSU process is almost done and the LCs are already running with the new firmware, so a failure when the previous AMM is upgrading would mean a reboot of the MM which restarts with the new image.

Global failures

ISSU is a very complex feature that includes many modules. If a fatal failure (e.g., an OS crash) happens in any MM during any stage of ISSU it would mean an ISSU abort and a system reboot. This is a fail forward scenario, where ISSU fails and the switch reboots to the new version. If the global error happens in the AMM, the error will be handled as fail forward. If the global error happens in the SMM before it is upgraded, the error will be handled as abort hitless. If the global error happens in the SMM after it was upgraded, the error will be handled as fail forward.

Configuration task list

The ISSU feature doesn't have many configuration tasks and it consists mainly of setting the system to a stable state and then triggering the ISSU process.

Pre-ISSU

1. Download the new image and store in the secondary bank.
2. Check management and line modules. The `show modules` command can be used for verification.

```
switch# show module

Management Modules
==================

     Product                                       Serial
Name Number  Description                           Number     Status
---- ------- ------------------------------------- ---------- ----------------
1/1  R0X31A  6400 Management Module                SG9ZKMG327 Active (local)
1/2  R0X31A  6400 Management Module                SG9ZKMG405 Standby


Line Modules
============

     Product                                       Serial
Name Number  Description                           Number     Status
---- ------- ------------------------------------- ---------- ----------------
1/3  R0X42A  6400 24p 10GT 4SFP56 Mod              SG0ZKMS156 Ready
1/4  R0X41A  6400 48p SR5 CL6 PoE 4SFP56 Mod       SG0ZKMR193 Ready
1/5  R0X39B  6400 48p 1GbE CL4 PoE 4SFP56 Mod      SG0ZKW2095 Ready
```

Start ISSU

The command to start the ISSU process is `issu update-software`:

```
switch# issu update-software

This command will perform an in-service software upgrade
using pre-staged secondary operating system image
FL.10.10.1000
This will save the current running configuration
```

```
Continue (y/n)? y

Starting in-service software upgrade.
```

Starting an ISSU will cause the running configuration to be saved in case an error is encountered that requires a reboot to recover the switch. Additionally, a special configuration checkpoint will be stored to disk, which can be used to go back to the pre-ISSU firmware. During the ISSU process all management methods (CLI, REST, WebUI) will be blocked from making configuration changes to the switch. Only non-config commands are allowed. The configuration block is active from the time ISSU starts until the time the ISSU failover is complete.

Troubleshooting

Once ISSU is started, it cannot be stopped. The current status of the ISSU process can be checked with the `show issu` and `show issu brief` commands.

In progress ISSU:

```
switch# show issu
ISSU Summary
============
ISSU Status     : In Progress
Current Version : FL.10.10.0001 Upgrade Version : FL.10.10.1000
Upgrade Image   : secondary          Start Date     : 2022-05-26 20:27:01
Last ISSU Result: -- (--)

ISSU Progress
=============
Upgrade Operation               Status         Start Date
----------------------------------------------------------------------
Initiate ISSU                   Complete       2022-05-26 20:27:01
Validate System Readiness       Complete       2022-05-26 20:27:01
Upgrade Standby Management Module  In Progress  2022-05-26 20:27:09
Upgrade Line Modules            Pending        --
Prepare for Switchover          Pending        --
Finalize Upgrade                Pending        --
ISSU Complete                   Pending        --
```

```
switch# show issu brief
ISSU Summary
============
ISSU Status     : In Progress
Current Version : FL.10.10.0001 Upgrade Version : FL.10.10.1000
Upgrade Image   : secondary          Start Date     : 2022-05-26 20:27:01
Last ISSU Result: -- (--)
```

Complete ISSU

```
switch# show issu
ISSU Summary
============
ISSU Status     : Ready
Current Version : FL.10.10.1000 Upgrade Version : --
Upgrade Image   : --                 Start Date     : --
```

```
Last ISSU Result: Completed (Without errors)

ISSU Progress
=============
Upgrade Operation               Status        Start Date
-------------------------------------------------------------------------------
Initiate ISSU                   Complete      2022-05-26 20:27:01
Validate System Readiness       Complete      2022-05-26 20:27:01
Upgrade Standby Management Module  Complete   2022-05-26 20:27:09
Upgrade Line Modules            Complete      2022-05-26 20:28:48
Prepare for Switchover          Complete      2022-05-26 20:30:21
Finalize Upgrade                Complete      2022-05-26 20:30:23
ISSU Complete                   Complete      2022-05-26 20:32:07
```

```
switch# show issu brief
ISSU Summary
============
ISSU Status     : Ready
Current Version : FL.10.11.0000-3140- Upgrade Version : --
Upgrade Image   : --                  Start Date      : --
Last ISSU Result: Completed (Without errors)
```

The output of these commands will show the current step in the ISSU process and the current state. E.g., if an error occurs and the error action taken.

There is also a debug command: `debug issu all severity debug`. This command will show information useful for troubleshooting and for technical support.

Frequently asked questions

Can ISSU be stopped?

Not currently.

What happens if a network event occurs during ISSU (e.g., a route reconvergence, a BFD update)?

Depending on the current ISSU step, these events could not be attended. Once ISSU is complete the system will start attending such events, but it is possible that some of them are missing. A network reconvergence may occur and possibly even some disruption (e.g., BFD blocking a port) is possible. It is important to note that all the limitations that apply to a regular failover apply to ISSU as well.

Can ISSU be performed between major versions?

Currently, ISSU is only supported to upgrade between minor versions. 10.10.0001 is the first release enabling ISSU support. ISSU is meant to be used to upgrade from this version to future minor releases.

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 a 6300 Series 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, a reboot will be required, though the hot-patch will still remain on the system. After the initial reboot, the disabled hot-patch can be removed from the system without the need for a second reboot.

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 Aruba 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.10.10.XXXX-YYYY.patch** indicates that the patch can be applied on top of switch image **FL.10.10.XXXX.swi** and brings software up to date with the **FL.10.10.YYYY** release.
- Hot-patch software can be applied only after it has been downloaded to the switch
- Hot-patch software can be applied to a standalone 6300 Series switch, or to a VSF stack of 6300 Series switches.

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.
- In order to fully deactivate or un-apply a hot-patch, a system reboot is required.
- 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.
- When multiple hot-patches are required, the first hot-patch should be removed after the second has been applied This includes hot-patches that are not compatible with the current running version of software. These 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.

To apply a hot-patch update

1. Request a hot-patch from Aruba 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 6300 Series 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 procedure for this option requires a reboot and the patch can be reapplied again since it is still on the device. If a previously unapplied patch needs to be removed/deleted the from the switch, it can be removed with the command **hot-patch remove <patch>.patch** and this will not need a second reboot.

```
6300(config)# show hot-patch
Name                                 Status
------------------------------------ ------
hpe-routing_FL_10_10_0001BJ.patch    Not applied
6300(config)# hot-patch apply hpe-routing_FL_10_10_0001BJ.patch
6300(config)#
6300(config)# show hot-patch
Name                                 Status
------------------------------------ ------
hpe-routing_FL_10_10_0001BJ.patch    Applied

6300(config)# no hot-patch apply hpe-routing_FL_10_10_0001BJ.patch

hpe-routing_FL_10_10_0001BJ.patch will remain applied until system reboots

Do you want to reboot now (y/n)? y
Checking if the configuration needs to be saved...
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.
The system is going down for reboot.
...

6300 login: admin
Password:
Last login: 2022-05-25 23:43:54 from the console
User "admin" has logged in 41 times in the past 30 days
6300#
6300# config
6300(config)#
6300(config)# show hot-patch
Name                                 Status
------------------------------------ ------
hpe-routing_FL_10_10_0001BJ.patch    Not applied

6300(config)#
6300(config)# hot-patch remove hpe-routing_FL_10_10_0001BJ.patch
Do you want to save the current configuration (y/n)? y
The running configuration was saved to the startup configuration.
6300(config)#
6300(config)# show hot-patch
No hot-patch found or configured
6300(config)#
```

To remove/delete a patch:

In this second option the patch is both unapplied and removed from the device completely. The patch cannot be reapplied unless it is downloaded again.

Use the **no hot-patch apply** command to disable the hot-patch image.

2. Use the **hot-patch remove** command to remove the patch image from the standalone

switch or VSF.

3. Reboot the switch or VSF system. When it comes up after the reboot, it will run the software version

it was using prior to the application of the patch update.

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

Restoring a checkpoint to a...	File type supported
Startup configuration	■ JSON ■ Checkpoint
Specified checkpoint	Specified checkpoint

Rollback

The term rollback is used to refer to when a switch configuration is reverted to a pre-existing checkpoint.

For example, the following command applies the configuration from checkpoint `ckpt1`. All previous configurations are lost after the execution of this command: `checkpoint rollback` *ckpt1*

You can also specify the rollback of the running configuration or of the startup configuration with a specified checkpoint, as shown with the following command: `copy checkpoint` *`<checkpoint-name>`* `{running-config | startup-config}`

Checkpoint auto mode

Checkpoint auto mode configures the switch with failover support, causing it to automatically revert to a previous configuration if it becomes inoperable or inaccessible due to configuration changes that are being made.

After entering checkpoint auto mode, you have a set amount of time to add, remove, or modify the existing switch configuration. To save your changes, you must execute the `checkpoint auto confirm` command before the auto mode timer expires. If you do not execute the `checkpoint auto confirm` command within the specified time, all configuration changes you made are discarded and the running configuration reverts to the state it was before entering checkpoint auto mode.

Testing a switch configuration in checkpoint auto mode

Process overview:

1. Enable the checkpoint auto mode.
2. To save the configuration, enter the `checkpoint auto confirm` command before the specified time set in step 1.

Checkpoint commands

checkpoint auto

`checkpoint auto <TIME-LAPSE-INTERVAL>`

Description

Starts auto checkpoint mode. In auto checkpoint mode, the switch temporarily saves the runtime configuration as a checkpoint only for the specified time lapse interval. Configuration changes must be saved before the interval expires, otherwise the runtime configuration is restored from the temporary checkpoint.

Parameter	Description
`<TIME-LAPSE-INTERVAL>`	Specifies the time lapse interval in minutes. Range: 1 to 60.

Usage

To save the runtime checkpoint permanently, run the `checkpoint auto confirm` command during the time lapse interval. The filename for the saved checkpoint is named `AUTO<YYYYMMDDHHMMSS>`. 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<YYYYMMDDHHMMSS>`. 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}
```

Description

Shows the difference in configuration between two configurations. Compare checkpoints, the running configuration, or the startup configuration.

Parameter	Description
{<CHECKPOINT-NAME1> | running-config | startup-config}	Selects either a checkpoint, the running configuration, or the startup configuration as the baseline.
{<CHECKPOINT-NAME2> | running-config | startup-config}	Selects either a checkpoint, the running configuration, or the startup configuration to compare.

Usability

The output of the `checkpoint diff` command has several symbols:

- The plus sign (+) at the beginning of a line indicates that the line exists in the comparison but not in the baseline.
- The minus sign (-) at the beginning of a line indicates that the line exists in the baseline but not in the comparison.

Examples

In the following example, the configurations of checkpoints `cp1` and `cp2` are displayed before the `checkpoint diff` command, so that you can see the context of the `checkpoint diff` command.

```
switch# show checkpoint cp1
Checkpoint configuration:
!
!Version AOS-CX XL.10.00.0002
!Schema version 0.1.8
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1,200
interface 1/1/1
    no shutdown
    ip address 1.0.0.1/24
interface 1/1/2
    no shutdown
    ip address 2.0.0.1/24

switch# show checkpoint cp2
Checkpoint configuration:
!
!Version AOS-CX XL.10.00.0002
!Schema version 0.1.8
module 1/1 product-number jl363a
!
!
!
!
!
!
!
vlan 1,200,300
interface 1/1/1
    no shutdown
    ip address 1.0.0.1/24
interface 1/1/2
    no shutdown
    ip address 2.0.0.1/24

switch# checkpoint diff cp1 cp2
--- /tmp/chkpt11501550258421    2017-08-01 01:17:38.420514016 +0000
+++ /tmp/chkpt21501550258421    2017-08-01 01:17:38.420514016 +0000
@@ -9,7 +9,7 @@
 !
 !
 !
-vlan 1,200
+vlan 1,200,300
 interface 1/1/1
     no shutdown
     ip address 1.0.0.1/24
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

checkpoint post-configuration

```
checkpoint post-configuration
```

```
no checkpoint post-configuration
```

Description

Enables creation of system generated checkpoints when configuration changes occur. This feature is enabled by default.

The `no` form of this command disables system generated checkpoints.

Usage

System generated checkpoints are automatically created by default. Whenever a configuration change occurs, the switch starts a timeout counter (300 seconds by default). For each additional configuration change, the timeout counter is restarted. If the timeout expires with no additional configuration changes being made, the switch generates a new checkpoint.

System generated checkpoints are named with the prefix `CPC` followed by a time stamp in the format `<YYYYMMDDHHMMSS>`. For example: `CPC20170630073127`.

System checkpoints can be applied using the checkpoint rollback feature or copy command.

A maximum of 32 system checkpoints can be created. Beyond this limit, the newest system checkpoint replaces the oldest system checkpoint.

Examples

Enabling system checkpoints:

```
switch(config)# checkpoint post-configuration
```

Disabling system checkpoints:

```
switch(config)# no checkpoint post-configuration
```

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.
<NEW-CHECKPOINT-NAME>	Specifies the new name for the checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-). **NOTE:** Do not start the checkpoint name with `CPC` because it is used for system-generated checkpoints.

Examples

Renaming checkpoint **ckpt1** to **cfg001**:

```
switch# checkpoint rename ckpt1 cfg001
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

checkpoint rollback

```
checkpoint rollback {<CHECKPOINT-NAME> | startup-config}
```

Description

Applies the configuration from a pre-existing checkpoint or the startup configuration to the running configuration.

Parameter	Description
<CHECKPOINT-NAME>	Specifies a checkpoint name.
`startup-config`	Specifies the startup configuration.

Examples

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

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

Applying a startup checkpoint to the running configuration:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy checkpoint *<CHECKPOINT-NAME> <REMOTE-URL>*

```
copy checkpoint <CHECKPOINT-NAME> <REMOTE-URL> [vrf <VRF-NAME>]
```

Description

Copies a checkpoint configuration to a remote location as a file. The configuration is exported in checkpoint format, which includes switch configuration and relevant metadata.

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

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

`vrf <VRF-NAME>`	Specifies a VRF name.

Examples

Copying checkpoint configuration to remote file through TFTP:

```
switch# copy checkpoint ckpt1 tftp://192.168.1.10/ckptmeta vrf default
################################################################### 100.0%
Success
```

Copying checkpoint configuration to remote file through SFTP:

```
switch# copy checkpoint ckpt1 sftp://root@192.168.1.10/ckptmeta vrf default
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ECDSA key fingerprint is SHA256:FtOm6Uxuxumil7VCwLnhz92H9LkjY+eURbdddOETy50.
Are you sure you want to continue connecting (yes/no)? yes
root@192.168.1.10's password:
sftp> put /tmp/ckptmeta ckptmeta
Uploading /tmp/ckptmeta to /root/ckptmeta
Warning: Permanently added '192.168.1.10' (ECDSA) to the list of known hosts.
Connected to 192.168.1.10.
Success
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy checkpoint *<CHECKPOINT-NAME>* {running-config | startup-config}

```
copy checkpoint <CHECKPOINT-NAME> {running-config | startup-config}
```

Description

Copies an existing checkpoint configuration to the running configuration or to the startup configuration.

Parameter	Description
`<CHECKPOINT-NAME>`	Specifies the name of an existing checkpoint.
`{running-config	startup-config}`	Selects whether the running configuration or the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration.

Examples

Copying **ckpt1** checkpoint to the running configuration:

```
switch# copy checkpoint ckpt1 running-config
Success
```

Copying **ckpt1** checkpoint to the startup configuration:

```
switch# copy checkpoint ckpt1 startup-config
Success
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy checkpoint *<CHECKPOINT-NAME>* *<STORAGE-URL>*

```
copy checkpoint <CHECKPOINT-NAME> <STORAGE-URL>
```

Description

Copies an existing checkpoint configuration to a USB drive. The file format is defined when the checkpoint was created.

Parameter	Description
<CHECKPOINT-NAME>	Specifies the name of the checkpoint to copy. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-).
<STORAGE-URL>>	Specifies the name of the target file on the USB drive using the following syntax: usb:/*<FILE>* The USB drive must be formatted with the FAT file system.

Examples

Copying the `test` checkpoint to the `testCheck` file on the USB drive:

```
switch# copy checkpoint test usb:/testCheck
Success
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy *<REMOTE-URL>* checkpoint *<CHECKPOINT-NAME>*

```
copy <REMOTE-URL> checkpoint <CHECKPOINT-NAME> [vrf <VRF-NAME>]
```

Description

Copies a remote configuration file to a checkpoint. The remote configuration file must be in checkpoint format.

Parameter	Description

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

`<CHECKPOINT-NAME>`	Specifies the name of the target checkpoint. The checkpoint name can be alphanumeric. It can also contain underscores (_) and dashes (-). Required. **NOTE:** Do not start the checkpoint name with `CPC` because it is used for system-generated checkpoints.
`vrf <VRF-NAME>`	Specifies a VRF name. Default: `default`.

Examples

Copying a checkpoint format file to checkpoint **ckpt5** on the default VRF:

```
switch# copy tftp://192.168.1.10/ckptmeta checkpoint ckpt5
################################################################## 100.0%
100.0%
Success
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy *<REMOTE-URL>* {running-config | startup-config}

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

Description

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

Parameter	Description

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

`{running-config	startup-config}`	Selects whether the running configuration or the startup configuration receives the copied checkpoint configuration. If the startup configuration is already present, the command overwrites the startup configuration.
`vrf <VRF-NAME>`	Specifies the name of a VRF. Default: default.

Usage

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

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

Examples

Copying a JSON format file to the running configuration:

```
switch# copy tftp://192.168.1.10/runjson running-config
######################################################################## 100.0%
Configuration may take several minutes to complete according to configuration file
size
 --0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Success
```

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

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

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
10.07 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 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

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> 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 or the copy will fail. the copy will not work.
startup-config	Specifies that the configuration file is copied to the startup configuration. The switch stores this configuration between reboots. The startup configuration is used as the operating configuration following a reboot of the switch. The file must be in JSON or checkpoint format or the copy will fail.
checkpoint *<CHECKPOINT-NAME>*	Specifies the name of a new checkpoint file to receive a copy of the configuration. The configuration file on the USB drive must be in checkpoint format. **NOTE:** Do not start the checkpoint name with CPC because it is used for system-generated checkpoints.

Usage

This command requires that the USB drive is formatted with the FAT file system and that the file be in the appropriate format as follows:

- `running-config`: This option requires the file on the USB drive be in CLI, JSON, or checkpoint format.
- `startup-config`: This option requires the file on the USB drive be in JSON or checkpoint format.
- `checkpoint <checkpoint-name>`: This option requires the file on the USB drive be in checkpoint format.

Examples

Copying the file **runCli** from the USB drive to the running configuration:

```
switch# copy usb:/runCli running-config
Configuration may take several minutes to complete according to configuration
file size
--0%----10%----20%----30%----40%----50%----60%----70%----80%----90%----100%--
Success
```

Copying the file **startUp** from the USB drive to the startup configuration:

```
switch# copy usb:/startUp startup-config
Success
```

Copying the file **testCheck** from the USB drive to the **abc** checkpoint:

```
switch# copy usb:/testCheck checkpoint abc
Success
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

erase

```
erase
    checkpoint <checkpont-name>
    core-dump all|daemon|dsm|kernel|vsf
    startup-config
    all
```

Description

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

Parameter	Description
`checkpoint <CHECKPOINT-NAME>`	Specifies the name of a checkpoint.
`core-dump all|daemon <daemon-name> |kernel|vsf`	Erase one of the following sets of core-dump files: ■ all: Erase all core-dump files. ■ daemon <daemon-name>: Erase daemon core-dump files. ■ kerne:l Erase the kernel core-dump. ■ vsf Erase daemon core-dump files for VSF. (For 6300 Switches only.)
`startup-config`	Specifies the startup configuration.
`all`	Specifies all checkpoints.

Examples

Erasing checkpoint **ckpt1**:

```
switch# erase checkpoint ckpt1
```

Erasing the startup configuration:

```
switch# erase startup-config
```

Erasing all checkpoints:

```
switch# erase checkpoint all
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show checkpoint *<CHECKPOINT-NAME>*

```
show checkpoint <CHECKPOINT-NAME> [json]
```

Description

Shows the configuration of a checkpoint.

Parameter	Description
<CHECKPOINT-NAME>	Specifies the name of a checkpoint.
[json]	Specifies that the output is displayed in JSON format.

Examples

Showing the configuration of the ckpt1 checkpoint in CLI format:

```
switch# show checkpoint ckpt1
Checkpoint configuration:
!
!Version AOS-CX PL.10.07.0000K-75-g55e5193
!export-password: default
lacp system-priority 65535
user admin group administrators password ciphertext
AQBapQjwipebv36io0jFfde7ZzrHckncal1D+3n8XFTZKQdmYgAAADEtYOeHSme93xzdD0uz6Vr9Kl+XBzB+
2GB0UBxSF7rvgN2x8KSgkqv7iqXVQ0Te6LkSMnH4BdNaT3Bf25qyvOqmr4YakO1V3rg8zAOADkPktQD8joTH
XflzwomoIzcmv/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.

Release	Modification
10.07 or earlier	--

Command Information

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

show checkpoint date

```
show checkpoint date <START-DATE> <END-DATE>
```

Description

Shows detailed list of all saved checkpoints created within the specified date range.

Parameter	Description
`<START-DATE>`	Specifies the starting date for the range of saved checkpoints to show. Format: `YYYY-MM-DD`.
`<END-DATE>`	Specifies the endingdate for the range of saved checkpoints to show. Format: `YYYY-MM-DD`.

Examples

Showing a detailed list of saved checkpoints for a specific date range:

```
switch# show checkpoint date 2017-03-08 2017-03-12

NAME              TYPE        WRITER  DATE(YYYY/MM/DD)        IMAGE VERSION
ckpt2             checkpoint  User    2017-03-08T18:10:01Z    XX.01.01.000X
ckpt3             checkpoint  User    2017-03-09T23:11:02Z    XX.01.01.000X
ckpt4             checkpoint  User    2017-03-11T00:00:03Z    XX.01.01.000X
```

Command History

Release	Modification
10.08	Command syntax `show checkpoint list date <START-DATE> <END-DATE>` is replaced with `show checkpoint date <START-DATE> <END-DATE>`
10.07 or earlier	--

Command Information

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

show running-config hash

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

Description

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

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

Examples

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

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

SHA-256 hash of the config in CLI format:

8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62aa1d715075b89e

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

Command History

Release	Modification
10.08	Command introduced

Command Information

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

show startup-config hash

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

Description

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

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

Examples

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

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

SHA-256 hash of the config in CLI format:

8db4e7e10f4b7f1a6ab17ad2b4efe0e72f1849103eaf43da62aa1d715075b89e

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

Command History

Release	Modification
10.08	Command introduced

Command Information

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

write memory

```
write memory
```

Description

Saves the running configuration to the startup configuration. It is an alias of the command `copy running-config startup-config`. If the startup configuration is already present, this command overwrites the startup configuration.

Examples

```
switch# write memory
Success
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Boot commands

boot 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
6300 6400	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

This command is supported on switches that have multiple line modules.

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
6300 6400	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
active	Selects the active management module.
standby	Selects the standby management module.
<SLOT-ID>	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 is supported on switches that have multiple management modules.

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
6300 6400	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 sets the configured default operating system image to primary for future reboots.
secondary	Selects the secondary operating system image for this reboot and sets the configured default operating system image to secondary for future reboots.
serviceos	Selects the service operating system for this reboot. Does not change the configured default operating system image. The service operating system acts as a standalone bootloader and recovery OS for switches running the AOS-CX operating system and is used in rare cases when troubleshooting a switch.

Usage

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

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

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

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

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

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

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

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

Examples

Rebooting the system from the configured default operating system image:

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

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

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]
```

Description

Shows boot information. When no parameters are specified, shows the most recent information about the boot operation, and the three previous boot operations for the active management module. When the `all` parameter is specified, shows the boot information for the active management module and all available line modules. To view boot-history on the standby, the command must be sent on the standby console.

Parameter	Description
all	Shows boot information for the active management module and all available line modules.

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.

`Index`
The position of the boot in the history file. Range: 0 to3.

`Boot ID`
A unique ID for the boot . A system-generated 128-bit string.

`Current Boot, up for <SECONDS> seconds`
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.

`Reboot requested through database`
The reboot occurred because of a request made through the CLI or other API.

`Uncontrolled reboot`
The reason for the reboot is not known.

Examples

Showing the boot history of the active management module:

```
switch# show boot-history
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
switch#
```

Showing the boot history of the active management module and all line modules:

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

`{hot-patch|primary|secondary}`	Select a hot-patch or a primary or secondary image profile for receiving the downloaded firmware. Required. **NOTE:** Hot patch software is supported on 6300 Series switches only. For more information, see hot-patch apply
`vrf <VRF-NAME>`	Specifies the name of a VRF. Default: default.

TFTP usage

To specify a URL with:

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

To specify TFTP with:

- the port number of the server in the URL: `tftp://192.0.2.1:12/a.txt`
- the blocksize in the URL: `tftp://192.0.2.1;blocksize=1462/a.txt`
  The valid blocksize range is 8 to 65464.
- the port number of the server and blocksize in the URL: `tftp://192.0.2.1:12;blocksize=1462/a.txt`

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

SFTP usage

To specify:

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

SCP Usage

To specify:

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

Examples

TFTP download for a hot-patch:

```
switch#  copy tftp://192.168.1.1/FL.10.10.0001-0002.patch hot-patch vrf vrf1

Fetching /users/swuser/FL.10.10.0001-0002.patch to hotpatch.dnld.uE2YT1
pbrd_FL_10_10_0001BA.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/ss.10.a0.0001.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/ss.10.00.0002.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
10.10	The `hot-patch` 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 secondary primary

```
copy secondary primary
```

Description

Copies the firmware image from the secondary to the primary location.

Examples

```
switch# copy secondary primary
The primary image will be deleted.

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

```
switch# copy sftp://stor@192.22.1.0/im-switch.swi primary vrf mgmt
The primary image will be deleted.

Continue (y/n)? y
The authenticity of host '192.22.1.0 (192.22.1.0)' can't be established.
ECDSA key fingerprint is SHA256:MyI1xbdKnehYut0NLfL69gDpNzCmZqBVvBaRR46m7o8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.22.1.0' (ECDSA) to the list of known hosts.
stor@192.22.1.0's password:
Connected to 192.22.1.0.
sftp> get c8d5b9f-topflite.swi c8d5b9f-topflite.swi.dnld
Fetching /home/dr/im-switch.swi to c8d5b9f-topflite.swi.dnld
/home/dr/im-switch.swi              100%  226MB  56.6MB/s   00:04

Verifying and writing system firmware...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

copy *<STORAGE-URL>*

```
copy <STORAGE-URL> {hot-patch|primary|secondary}
```

Description

Copies, verifies, and installs a hot-patch or firmware image from a USB storage device connected to the active management module.

Parameter	Description
<STORAGE-URL>	Specifies the name of the firmware file to copy from the storage device. Required. **USB format:** usb:/*<FILENAME>*
{hot-patch|primary|secondary}	Select a hot-patch image or a primary or secondary profile for receiving the copied firmware. **NOTE:** hot-patch images are supported by 6300 Series switches only. For more information, see hot-patch apply

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.10.01.0001-0002.patch
```

```
switch# copy usb:/11.10.00.0002.swi primary
The primary image will be deleted.

Continue (y/n)? y

Verifying and writing system firmware...
```

Command History

Release	Modification
10.10	The hot-patch 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 hot-patch

```
copy hot-patch <word> {<REMOTE-URL>|<Storage-URL>} [vrf <VRF-NAME>]
```

Description

Copies a hot-patch from a 6300 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_10_0001-0002.patch`. For information on how to format the path to a firmware file on a USB drive, see USB URL.

Examples

```
switch# copy hot-patch FL_10_10_0001-0002.patch tftp:172.21.18.170/FL_10_10_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	Apply a hot-patch image or remove it from the switch.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Administrators or local user group members with execution rights for this command.

hot-patch apply

```
hot-patch apply|remove <name.patch>
no hot-patch apply <name.patch>
```

Description

Apply a hot-patch 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.

Profile names	Description
`apply <name.patch>`	Apply the specified hot-patch image to a standalone 6300 Series switch or VRF stack. AOS-CX hot-patch software images can be obtained from Aruba customer support, and are identified with a **.patch** extension.
`remove <name.patch>`	Ater you have disabled a hot-patch image with the `no hot-patch apply <name.patch>` command, use the `hot-patch remove <name.patch>` command to remove the patch from the server.

Usage

A hot-patch can be downloaded from a remote server onto a 6300 Series switch then applied without rebooting the switch. When the hot-patch is disabled, a reboot will be required, though the hot-patch will still remain on the system. After the initial reboot, the disabled hot-patch can be removed from the system by without the need for a second reboot.

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's memory.

Examples

```
switch(config)# hot-patch apply FL_10_10_0001-0002.patch
```

Related Commands

Command	Description
copy <REMOTE-URL>	Downloads and installs a hot-patch image from a TFTP or SFTP server to a 6300 Series switch.
copy hot-patch	Copies a hot-patch software image from a 6300 Series switch to a specified remote URL or storage URL.

Command History

Release	Modification
10.10	Command introduced.

Command Information

Platforms	Command context	Authority
6300	`config`	Administrators or local user group members with execution rights for this command.

issu update-software

```
issu update-software
```

Description

Initiates an in-service software upgrade (ISSU) to the alternate boot location.

Usage

Note the following points before running this command:

- The newer operating system image must be downloaded to the alternate boot location prior to running this command.
- The current running operating system version must match the version that is stored in the current boot location or ISSU will not be allowed.
- This operation is disruptive and will result in the management interface being disconnected during the process.
- The running configuration will be stored in case an error is encountered that requires a reboot to recover the switch.
- During the ISSU process all management methods (CLI, REST, WebUI) are blocked from making configuration changes to the switch. The configuration changes are not allowed from the time ISSU starts until ISSU switchover is complete. After the ISSU switchover completes, the newly upgraded alternate management module is actived and switch configuration is resumed.

Examples

Initiate an in-service software upgrade.

```
switch(config)# issu update-software

This command will perform an in-service software upgrade
using the pre-staged secondary operating system image
FL.10.10.0002

Continue (y/n)? y

switch#
```

Initiate an in-service software upgrade but halt without confirming the upgrade.

```
switch(config)# issu update-software
```

```
This command will perform an in-service software upgrade
using the pre-staged primary operating system image
FL.10.10.0002

Continue (y/n)? n
In-service software upgrade aborted. No changes were made.

switch#
```

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
6400	`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 an applied hot-patch

Examples

```
switch# show hot-patch

Name                            Status
----------------------          -------
FL_10_10_0001-0002.patch        Applied

switch# show hot-patch detail

Name               : FL_10_10_0001-0002.patch
Status             : Applied
Version            : FL_10_10_0001-0002.patch
Compatible Version : FL.10.10.0001
Issues Fixed       : CR1234, CR2345
Patch Date         : 2022-03-29 20:46:15 UTC
Patch ID           : ArubaOS-CX:FL.10.10.0001-sp1-256-gd457e868d39:202204142009
Patch SHA          : a40438d06a82e5fe7e30d457e868d39e8526185b
```

The * symbol by a hot-patch name in the output of this comand, that indicates that the hot-patch is disabled but is still active on the switch. A disabled hot-patch remains active or applied on the system until it reboots.

```
switch# show hot-patch

Name                            Status
-----------------------         -------
ztpd.patch                      *Applied
```

Related Commands

Command	Description
copy <REMOTE-URL>	Downloads a hot-patch image from a TFTP or SFTP server.
hot-patch apply	Apply a hot-patch image or remove it from the switch.

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
6300	Manager (#)	Administrators or local user group members with execution rights for this command.

show issu

```
show issu [brief]
```

Description

Shows information about the current state of ISSU. If no ISSU is currently in progress, the command displays the progress details of the last ISSU.

The command with the `brief` parameter displays a short summary of the ISSU state and indicates if the system is ready to accept an ISSU command and whether or not an ISSU is in progress. If the `brief` parameter is not included, then more details about an in progress ISSU or the last ISSU are displayed.

Parameter	Description
brief	Shows a short summary of the ISSU state.

Examples

Show detailed ISSU status with ISSU in progress for the first time.

```
switch# show issu
ISSU Summary
===========
ISSU Status     : In progress
Current Version : FL.10.10.0001     Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary        Start Date      : 2021-10-15 08:37:49
Last ISSU Result: -- (--)

ISSU Progress
=============
Upgrade Operation                 Status        Start Date
----------------------------------------------------------------------------
Initiate ISSU                     Complete      2021-10-13 23:05:41
Validate System Readiness         Complete      2021-10-13 23:05:41
Upgrade Standby Management Module Complete      2021-10-13 23:05:41
Upgrade Line Modules              In Progress   2021-10-13 23:07:07
Prepare for Switchover            Pending       --
Perform Switchover                Pending       --
Finalize Upgrade                  Pending       --
ISSU Complete                     Pending       --
```

Show detailed ISSU status with ISSU in progress after successfully completing a previous ISSU.

```
switch# show issu
ISSU Summary
===========
ISSU Status     : In progress
Current Version : FL.10.10.0001     Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary        Start Date      : 2021-10-15 08:37:49
Last ISSU Result: Completed (Without errors)

ISSU Progress
=============
Upgrade Operation                 Status        Start Date
----------------------------------------------------------------------------
Initiate ISSU                     Complete      2021-10-13 23:05:41
Validate System Readiness         Complete      2021-10-13 23:05:41
Upgrade Standby Management Module Complete      2021-10-13 23:05:41
Upgrade Line Modules              In Progress   2021-10-13 23:07:07
Prepare for Switchover            Pending       --
Perform Switchover                Pending       --
Finalize Upgrade                  Pending       --
ISSU Complete                     Pending       --
```

Show detailed ISSU status with ISSU in progress after aborting the previous ISSU.

```
switch# show issu
ISSU Summary
===========
ISSU Status     : In progress
Current Version : FL.10.10.0001     Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary        Start Date      : 2021-10-15 08:37:49
Last ISSU Result: Aborted (One or more line modules are not ready to start ISSU)

ISSU Progress
=============
Upgrade Operation                 Status        Start Date
----------------------------------------------------------------------------
Initiate ISSU                     Complete      2021-10-13 23:05:41
```

```
Validate System Readiness          Complete       2021-10-13 23:05:41
Upgrade Standby Management Module   Complete       2021-10-13 23:05:41
Upgrade Line Modules                In Progress    2021-10-13 23:07:07
Prepare for Switchover              Pending        --
Perform Switchover                  Pending        --
Finalize Upgrade                    Pending        --
ISSU Complete                       Pending        --
```

Show detailed ISSU status with no ISSU in progress and no previous ISSU performed.

```
switch# show issu
ISSU Summary
===========
ISSU Status    : Ready
Current Version : FL.10.10.0001     Upgrade Version : --
Upgrade Image   : --                Start Date      : --
Last ISSU Result: -- (--)

ISSU Progress
=============
Upgrade Operation              Status        Start Date
-------------------------------------------------------------------------
Initiate ISSU                  --            --
Validate System Readiness      --            --
Upgrade Standby Management Module  --        --
Upgrade Line Modules           --            --
Prepare for Switchover         --            --
Perform Switchover             --            --
Finalize Upgrade               --            --
ISSU Complete                  --            --
```

Show detailed ISSU status after completion and before system is ready to start a new ISSU.

```
switch# show issu
ISSU Summary
===========
ISSU Status    : Not ready
Current Version : FL.10.10.0001     Upgrade Version : --
Upgrade Image   : --                Start Date      : --
Last ISSU Result: Completed (Without errors)

ISSU Progress
=============
Upgrade Operation              Status        Start Date
-------------------------------------------------------------------------
Initiate ISSU                  Complete      2021-10-13 23:05:41
Validate System Readiness      Complete      2021-10-13 23:05:41
Upgrade Standby Management Module  Complete  2021-10-13 23:05:41
Upgrade Line Modules           Complete      2021-10-13 23:07:07
Prepare for Switchover         Complete      2021-10-13 23:07:50
Finalize Upgrade               Complete      2021-10-13 23:07:53
ISSU Complete                  Complete      2021-10-13 23:08:10
```

Show detailed ISSU status after an error occurred and the process is aborted.

```
switch# show issu
ISSU Summary
```

```
============
ISSU Status     : Aborted
Current Version : FL.10.10.0001      Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary          Start Date      : 2021-12-09 19:17:15
Last ISSU Result: Aborted (System failed to prepare for ISSU)


ISSU Progress
=============
Upgrade Operation               Status        Start Date
--------------------------------------------------------------------------
Initiate ISSU                   Complete      2021-12-09 19:17:15
Validate System Readiness       Complete      2021-12-09 19:17:15
Upgrade Standby Management Module Complete    2021-12-09 19:17:15
Upgrade Line Modules            Error         2021-12-09 19:19:22
Prepare for Switchover          Aborted       --
Finalize Upgrade                Aborted       --
ISSU Complete                   Aborted       --
```

Show summary of ISSU status with no ISSU in progress, where system is ready to start a new ISSU, with no previous ISSU performed.

```
switch# show issu brief
ISSU Summary
===========
ISSU Status     : Ready
Current Version : FL.10.10.0001      Upgrade Version : --
Upgrade Image   : --                 Start Date      : --
Last ISSU Result: -- (--)
```

Show summary of ISSU status with no ISSU in progress, where system is ready to start a new ISSU, after successfully completing a previous ISSU.

```
switch# show issu brief
ISSU Summary
===========
ISSU Status     : Ready
Current Version : FL.10.10.0001      Upgrade Version : --
Upgrade Image   : --                 Start Date      : --
Last ISSU Result: Completed (Without errors)
```

Show summary of ISSU status with no ISSU in progress, where system is ready to start a new ISSU, after aborting the previous ISSU.

```
switch# show issu brief
ISSU Summary
===========
ISSU Status     : Ready
Current Version : FL.10.10.0001      Upgrade Version : --
Upgrade Image   : --                 Start Date      : --
Last ISSU Result: Aborted (One or more line modules are not ready to start ISSU)
```

Show summary of ISSU status with ISSU in progress.

```
switch# show issu brief
ISSU Summary
```

```
===========
ISSU Status      : In progress
Current Version : FL.10.10.0001      Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary          Start Date      : 2021-10-15 08:37:49
Last ISSU Result: Completed (Without errors)
```

Show summary of ISSU status with no ISSU in progress where the system is not ready to start a new ISSU.

```
switch# show issu brief
ISSU Summary
===========
ISSU Status      : Not ready
Current Version : FL.10.10.0001      Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary          Start Date      : 2021-10-15 08:37:49
Last ISSU Result: Completed (Without errors)
```

Show summary of ISSU status after an error occurred and the process is aborted.

```
switch# show issu brief
ISSU Summary
============
ISSU Status      : Aborted
Current Version : FL.10.10.0001       Upgrade Version : FL.10.10.0002
Upgrade Image   : secondary           Start Date      : 2021-12-09 19:17:15
Last ISSU Result: Aborted (System failed to prepare for ISSU)
```

Command History

Release	Modification
10.10	Command introduced

Command Information

Platforms	Command context	Authority
6400	Manager (#)	Administrators or local user group members with execution rights for this command.

For information on dynamic segmentation, view the *Security Guide*.

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.

The Aruba Central network management solution, a software-as-a-service subscription in the cloud, provides streamlined management of multiple network devices. AOS-CX switches are able to talk to Aruba Central and utilize cloud-based management functionality. Cloud-based management functionality allows for the deployment of network devices at sites with no or few dedicated IT personnel (branch offices, retail stores, and so forth). AOS-CX switches utilize secure communication protocols to connect to the Aruba Central cloud portal, and can coexist with corporate security standards, such as those mandating the use of firewalls.

> When Aruba Central manages AOS-CX switches, it functions as the single source of truth and the Web UI operates in read-only mode.

This feature provides:

- Zero-touch provisioning
- Network Management/Remote monitoring
- Events/alerts notification
- Switch Configuration using templates
- Firmware management

Connecting to Aruba Central

AOS-CX switch downloads the location of Aruba Central server using:

- Command-line interface (CLI).
- Aruba Activate server.
- DHCP options provided during ZTP.

DHCP servers are used to connect to Central on-premise management.

If switch is unable to connect to Activate server, it retries to establish connection in exponential back off of 1s, 2s, 8s, 16s, 32s, 64s, 128s, and 256s. After the maximum back off of 256s, switch retries happen for every 5 minutes.

> If the Network Time Protocol (NTP) is not enabled on the switch, it will synchronize the system time with the Activate server.

Custom CA certificate

To use custom CA certificate to connect to Aruba Central, AOS-CX switch downloads the certificate from Aruba Activate server.

- If there is no custom CA provided by Aruba Activate, the CA certificate present in the device is used.
- Duplicate CA certificates from Aruba Activate server will be ignored.
- If CA certificate is absent in consecutive responses from Aruba Activate server, the installed custom CA certificate in device will be removed.
- Switch will have only one custom CA certificate installed from Aruba Activate Server.
- The certificate installed from Aruba Activate server will not be displayed in the show commands.

Support mode in Aruba Central

When the AOS-CX switch is managed by Aruba Central, the switch configuration cannot be modified using other interfaces such as CLI or Web UI. The following command categories are blocked:

- auto-confirm
- boot
- checkpoint
- copy-in commands
- erase
- erps
- https-server
- mfgread
- mfgwrite
- port-access
- vsf
- All configuration commands except the aruba-central command

In cases where a maintenance or troubleshooting activity requires configuration updates, aruba-central support-mode can be enabled to allow these operations.

The aruba-central support-mode enable or disable operation is effective only in the CLI session where it is executed and does not impact the other CLI sessions.

If the user tries to execute any command that is not allowed, an **Invalid input:** error message is displayed.

Aruba Central commands

aruba-central

```
aruba-central
no aruba-central
```

Description

Creates or enters the Aruba Central configuration context (`config-aruba-central`).

Example

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

Creating the Aruba Central configuration context:

```
switch(config)# aruba-central
switch(config-aruba-central)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

aruba-central support-mode

```
aruba-central support-mode
no aruba-central support-mode
```

Description

Allows the device to be writable for all operations in Aruba Central lockout mode for troubleshooting. The no form of this command disables this activity.

> Support-mode is disabled by default when the switch is managed by Aruba Central. This command is only effective in the CLI session where it is executed.

Examples

Configuring the device to be writable for all operations in Aruba Central lockout mode:

```
switch# aruba-central support-mode
switch#
```

Removing the configuration that allows the device to be writable for all operations in Aruba Central lockout mode:

```
switch# no aruba-central support-mode
switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Manager (#)	Administrators or local user group members with execution rights for this command.

configuration-lockout central managed

```
configuration-lockout central managed
no configuration-lockout central managed
```

Description

Configures the device to only be writable from Aruba Central. Aruba Central will be the only agent that can add, modify, or delete configurations on the device. The no form of this command disables this feature.

> The no form of this command is only available when the device is disconnected from Aruba Central.

Usage

The AOS-CX switch connects to Aruba Central in either of two modes: monitor or managed. When the device is connected in monitor mode, Aruba Central monitors the configurations on the switch. When the device is connected in managed mode, the `configuration-lockout central managed` command does not allow configuration changes from other interfaces such as CLI or Web UI.

Examples

Configuring the device to only be writable from Aruba Central :

```
switch(config)# configuration-lockout central managed
switch# show configuration-lockout
configuration lockout
--------------------
central: managed
switch# sh aruba-central
Central admin state                 :enable
Central location                    :20.0.0.2:8083
VRF for connection                  :default
Central connection status           :connected

Central source                      :cli
Central source connection status    :connected
Central source last connected on    :Tue Feb 9 17:53:13 UTC 2021

Activate Server URL                 :devices-v2.arubanetworks.com
CLI location                        :20.0.2:8083
CLI VRF                             :default
switch(config)# end
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

disable

`disable`

Description

Disables connection to Aruba Central server.

When the connection is disabled, the switch does not attempt to connect to the Aruba Central server or fetch central location from any of the three sources (CLI/Aruba Activate/DHCP). It also disconnects any active connection to the Aruba Central server.

Example

```
switch(config-aruba-central)# disable
switch(config-aruba-central)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-aruba-central`	Administrators or local user group members with execution rights for this command.

enable

`enable`

Description

Enables connection to Aruba Central server. When the connection is enabled, the switch attempts to download the location of the Aruba Central server in one of the following ways at startup and after the connection is lost:

- Using command-line interface (CLI).
- Connecting to Aruba Activate server.
- Using DHCP options provided during ZTP.

DHCP servers provide the options requested by the device to connect to Central, Central On-premise managment, or the TFTP server.

Examples

```
switch(config-aruba-central)# enable
switch(config-aruba-central)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-aruba-central`	Administrators or local user group members with execution rights for this command.

location-override

```
location-override <location> [vrf <VRF-NAME>]
no location-override
```

Description

When `location` and `vrf` are configured, the switch overrides existing connections to Aruba Central. The switch attempts to establish connection to Aruba Central with the specified location and VRF with highest priority.

The `no` form of this command removes location override values from the Aruba Central configuration context.

Parameter	Description
`<location>`	Specifies one of these values: ■ `<FQDN>`: a fully qualified domain name. ■ `<IPV4>`: an IPv4 address. ■ `<IPV6>`: an IPv6 address.
`vrf <VRF-NAME>`	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named `default` is used.

Examples

Configuring location override with location and VRF:

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

Configuring location override with location only:

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

Removing location override values from the Aruba Central configuration context:

```
switch(config-aruba-central)# no location-override
switch(config-aruba-central)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	config-aruba-central	Administrators or local user group members with execution rights for this command.

show aruba-central

```
show aruba-central
```

Description

Shows information about Aruba Central connection and the status of the Activate server connection.

Examples

Example of a switch that has the Aruba Central connection:

```
switch# show aruba-central
Central admin state                    :enabled
Central location                       : N/A
VRF for connection                     : N/A
Central connection status              : N/A
Central source                         : dhcp
Central source connection status       : connection_failure
Central source last connected on       : N/A
System time synchronized from Activate : True
Activate server URL                    : 172.17.0.1
CLI location                           : N/A
CLI VRF                                : N/A
Source IP                              : N/A
Source IP Overridden                   : false
Central support mode                   : disabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config current-context

```
show running-config current-context
```

Description

Shows the running configuration for the current-context. If user is in the context of Aruba-Central(`config-aruba-central`), then Aruba Central running configuration is displayed.

Examples

Shows the running configuration of Aruba Central:

```
switch(config-aruba-central)# show running-config current-context
aruba-central
        disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Port 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 5 *Port Filter Application*

Configuring a port filter to drop traffic received on port 1/1/1 with an outbound destination of port 1/1/2 means that End Nodes A, B, and C cannot send traffic to the server. To block traffic in the opposite direction, you would also configure a port filter to drop traffic received on port 1/1/2 with an outbound destination of port 1/1/1.

;" />
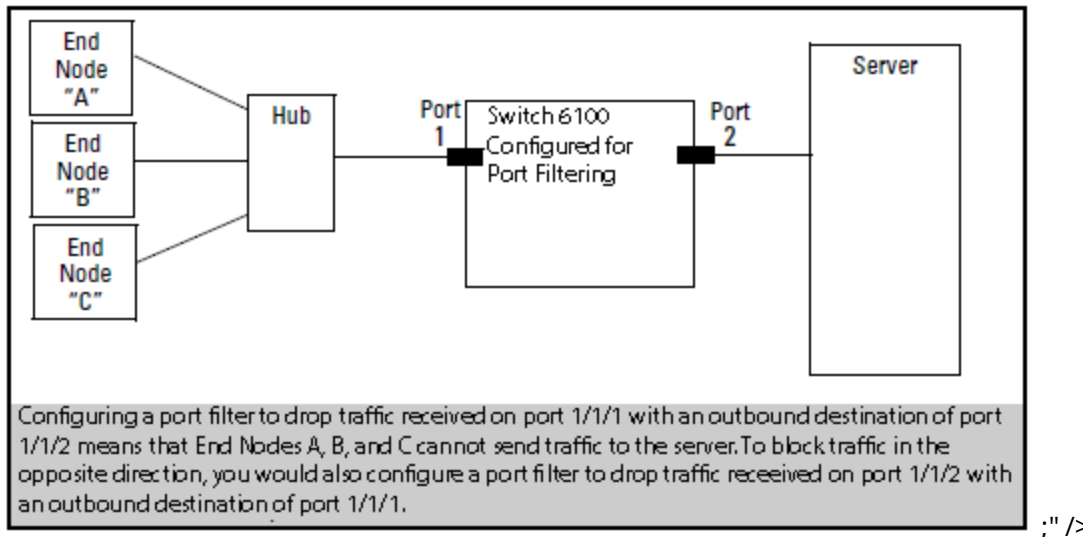
Port filtering commands

portfilter

```
portfilter <INTERFACE-LIST>
no portfilter [<INTERFACE-LIST>]
```

Description

Configures the specified ports so they do not egress any packets that were received on the source port specified in interface context.

The `no` form of this command removes the port filter setting from one or more ingress ports/LAGs.

Parameter	Description
`<INTERFACE-LIST>`	Specifies a list of ports/LAGs to be blocked for egressing. Specify a single interface or LAG, or a range as a comma-separated list, or both. For example: `1/1/1`, `1/1/3-1/1/6`,`lag2`, `lag1-lag4`. *On the 6400 Switch Series, interface identification differs.*

Usage

When a port filter configuration is applied on the same ingress physical port/LAG, the configuration is updated with the new sets of egress ports/LAGs that are to be blocked for egressing and that are not a part of its previous configuration. Duplicate updates on an existing port filter configuration are ignored.

When egress ports/LAGs are removed from the existing port filter configuration of an ingress port/LAG, egressing is allowed again on those egress ports/LAGs for all packets originating from the ingress port/LAG.

The `no portfilter [<IF-NAME-LIST>]` command removes port filter configurations from the egress ports/LAGs listed in the *<IF-NAME-LIST>* parameter only. All other egress ports/LAGs in the port filter configuration of the ingress port/LAG remain intact.

If no physical ports or LAGs are provided for the `no portfilter` command, the command removes the entire port filter configuration for the ingress port/LAG.

Examples

On the 6400 Switch Series, interface identification differs.

Creating a filter that prevents packets received on port **1/1/1** from forwarding to ports **1/1/3-1/1/6** and to LAGs **1** through **4**:

```
switch(config)# interface 1/1/1
switch(config-if)# portfilter 1/1/3-1/1/6,lag1-lag4
```

Creating a filter that prevents packets received on LAG **1** from forwarding to ports **1/1/6** and LAGs **2** and **4**:

```
switch(config)# interface lag 1
switch(config-lag-if)# portfilter 1/1/6,lag2,lag4
```

Removing filters from an existing configuration that allows back packets received on port **1/1/1** to forward to ports **1/1/6** and LAGs **3** and **4**:

```
switch(config)# interface 1/1/1
switch(config-if)# no portfilter 1/1/6,lag3,lag4
```

Removing all filters from an existing configuration that allows back packets received on LAG **1** to forward to all the ports and LAGs:

```
switch(config)# interface lag 1
switch(config-lag-if)# no portfilter
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show portfilter

```
show portfilter [<IFNAME>][vsx-peer]
```

Description

Displays filter settings for all interfaces or a specific interface.

Parameter	Description
<IFNAME>	Specifies the ingress interface name. Specifies one of these values: ■ *<FQDN>*: a fully qualified domain name. ■ *<IPV4>*: an IPv4 address. ■ *<IPV6>*: an IPv6 address.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

On the 6400 Switch Series, interface identification differs.

Displaying all port filter settings on the switch:

```
switch# show portfilter
Incoming    Blocked
Interface   Outgoing Interfaces
-------------------------------------------------------------------------------
1/1/1       1/1/3-1/1/6,lag1-lag2
1/1/3       1/1/1,1/1/5,1/1/7,1/1/9,1/1/11,1/1/13,1/1/15,1/1/17,1/1/19,1/1/21,
            1/1/23,1/1/25,1/1/27,1/1/29,1/1/31,1/1/33,1/1/35
lag2        1/1/1,1/1/3-1/1/6
```

Displaying the port filter settings for port **1/1/1**:

```
switch# show portfilter 1/1/1
Incoming    Blocked
Interface   Outgoing Interfaces
-------------------------------------------------------------------------------
1/1/1       1/1/3-1/1/6,lag1-lag2
```

Displaying the port filter settings for **LAG2**:

```
switch# show portfilter lag2
Incoming    Blocked
Interface   Outgoing Interfaces
-------------------------------------------------------------------------------
lag2        1/1/1,1/1/3-1/1/6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	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 Domain Name System (DNS) is the Internet protocol for mapping a hostname to its IP address. 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.

DNS client

The DNS client resolves hostnames to IP addresses for protocols that are running on the switch. When the DNS client receives a request to resolve a hostname, it can do so in one of two ways:

- Forward the request to a DNS name server for resolution.
- Reply to the request without using a DNS name server, by resolving the name using a statically defined table of hostnames and their associated IP addresses.

Configuring the DNS client

Procedure

1. Configure one or more DNS name servers with the command `ip dns server`.
2. To resolve DNS requests by appending a domain name to the requests, either configure a single domain name with the command `ip dns domain-name`, or configure a list of up to six domain names with the command `ip dns domain-list`.
3. To use static name resolution for certain hosts, associate an IP address to a host with the command `ip dns host`.
4. Review your DNS configuration settings with the command `show ip dns`.

Examples

This example creates the following configuration:

- Defines the domain **switch.com** to append to all requests.
- Defines a DNS server with IPv4 address of **1.1.1.1**.
- Defines a static DNS host named **myhost1** with an IPv4 address of **3.3.3.3**.
- DNS client traffic is sent on the default VRF (named **default**).

```
switch(config)# ip dns domain-name switch.com
switch(config)# ip dns server-address 1.1.1.1
switch(config)# ip dns host myhost1 3.3.3.3
switch(config)# exit
switch# show ip dns

VRF Name : vrf_mgmt

Host Name                                                    Address
------------------------------------------------------------------------------


VRF Name : vrf_default
Domain Name : switch.com
DNS Domain list :
Name Server(s) : 1.1.1.1

Host Name                                                    Address
------------------------------------------------------------------------------
myhost1
```

This example creates the following configuration:

- Defines three domains to append to DNS requests **domain1.com**, **domain2.com**, **domain3.com** with traffic forwarding on VRF **mainvrf**.
- Defines a DNS server with an IPv6 address of **c::13**.
- Defines a DNS host named **myhost** with an IPv4 address of **3.3.3.3**.

```
switch(config)# ip dns domain-list domain1.com vrf mainvrf
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain3.com vrf mainvrf
switch(config)# ip dns server-address c::13
switch(config)# ip dns host myhost 3.3.3.3 vrf mainvrf
switch(config)# quit
switch# show ip dns mainvrf

VRF Name : mainvrf
Domain Name :
DNS Domain list : domain1.com, domain2.com, domain3.com
Name Server(s) : c::13

Host Name                                                    Address
------------------------------------------------------------------------------
myhost                                                       3.3.3.3
```

DNS client commands

ip dns domain-list

```
ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
no ip dns domain-list <DOMAIN-NAME> [vrf <VRF-NAME>]
```

Description

Configures one or more domain names that are appended to the DNS request. The DNS client appends each name in succession until the DNS server replies. Domains can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF.

The `no` form of this command removes a domain from the list.

Parameter	Description
`list <DOMAIN-NAME>`	Specifies a domain name. Up to six domains can be added to the list. Length: 1 to 256 characters.
`vrf <VRF-NAME>`	Specifies a VRF name. Default: default.

Examples

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

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

This example defines a list with two entries, **domain2.com** and **domain5.com**, with requests being sent on **mainvrf**.

```
switch(config)# ip dns domain-list domain2.com vrf mainvrf
switch(config)# ip dns domain-list domain5.com vrf mainvrf
```

This example removes the entry **domain1.com**.

```
switch(config)# no ip dns domain-list domain1.com
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip dns domain-name

```
ip dns domain-name <DOMAIN-NAME> [ vrf <VRF-NAME> ]
no ip dns domain-name <DOMAIN-NAME> [ vrf <VRF-NAME> ]
```

Description

Configures a domain name that is appended to the DNS request. The domain can be either IPv4 or IPv6. By default, requests are forwarded on the default VRF. If a domain list is defined with the command `ip dns domain-list`, the domain name defined with this command is ignored.

The `no` form of this command removes the domain name.

Parameter	Description
`<DOMAIN-NAME>`	Specifies the domain name to append to DNS requests. Length: 1 to 256 characters.
`vrf <VRF-NAME>`	Specifies a VRF name. Default: default.

Examples

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

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

Removing the default domain name `domain.com`:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip dns host

```
ip dns host <HOST-NAME> <IP-ADDR> [ vrf <VRF-NAME> ]
no ip dns host <HOST-NAME> <IP-ADDR> [ vrf <VRF-NAME> ]
```

Description

Associates a static IP address with a hostname. The DNS client returns this IP address instead of querying a DNS server for an IP address for the hostname. Up to six hosts can be defined. If no VRF is defined, the default VRF is used.

The `no` form of this command removes a static IP address associated with a hostname.

Parameter	Description
`host <HOST-NAME>`	Specifies the name of a host. Length: 1 to 256 characters.
`<IP-ADDR>`	Specifies an IP address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255, or IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.
`vrf <VRF-NAME>`	Specifies a VRF name. Default: default.

Examples

This example defines an IPv4 address of **3.3.3.3** for **host1**.

```
switch(config)# ip dns host host1 3.3.3.3
```

This example defines an IPv6 address of **b::5** for **host 1**.

```
switch(config)# ip dns host host1 b::5
```

This example defines removes the entry for **host 1** with address **b::5**.

```
switch(config)# no ip dns host host1 b::5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

ip dns server address

```
ip dns server-address <IP-ADDR> [ vrf <VRF-NAME> ]
no ip dns server-address <IP-ADDR> [ vrf <VRF-NAME> ]
```

Description

Configures the DNS name servers that the DNS client queries to resolve DNS queries. Up to six name servers can be defined. The DNS client queries the servers in the order that they are defined. If no VRF is defined, the default VRF is used.

The `no` form of this command removes a name server from the list.

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

Examples

This example defines a name server at **1.1.1.1**.

```
switch(config)# ip dns server-address 1.1.1.1
```

This example defines a name server at **a::1**.

```
switch(config)# ip dns server-address a::1
```

This example removes a name server at **a::1**.

```
switch(config)# no ip dns server-address a::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show ip dns

```
show ip dns [vrf <VRF-NAME>][vsx-peer]
```

Description

Shows all DNS client configuration settings or the settings for a specific VRF.

Parameter	Description
vrf <VRF-NAME>	Specifies the VRF for which to show information. If no VRF is defined, the default VRF is used.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

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, CDP, and local MAC match by using device profiles to enable automatic discovery and configuration of other devices on the network.

Based on the type of devices connected to the interface, device profiles enable predefined configurations that can be applied to the interface. Connected devices are identified using corresponding protocol packets. When the protocol information on the interface ages, the profile or role is revoked from the interface. Only devices connected directly to the switch are detected and processed to apply a device profile. When a device of a configured type is connected to an interface, the switch automatically applies the corresponding Device profiles .

Local MAC match enables dynamic assignment of client attributes, such QoS and VLANs by using a locally configured authentication repository. Local MAC match involves creating MAC groups that are used to classify connected devices based on MAC address, MAC address mask, and MAC OUI. Local MAC match feature is useful when you do not want to afford RADIUS infrastructure or when you want to use local authentication as a backup method in case the RADIUS server is unreachable.

The following parameters can be configured for each role:

- `associate:` Used to associate captive-portal-profile or policy with the role.
- `auth-mode:` Used to configure authentication mode for the role.

> There is no need to configure `auth-mode` for a plain device profile.

- `mtu:` Used to configure MTU for the role.
- `poe-priority:` Used to configure the PoE priority for the role.
- `trust-mode:` Used to configure trust mode for the role.
- `vlan:` Used to configure VLAN mode for the role.
- `stp-admin-edge-port:` Used to configure STP administrative edge port for the role.

For information on role configurations, see the *Security Guide*.

> The following commands are not supported in local MAC match feature:
> - `aaa authentication port-access mac-auth cached-reauth`
> - `aaa authentication port-access mac-auth cached-reauth-period`
> - `aaa authentication port-access mac-auth quiet-period`
> - `aaa authentication port-access mac-auth reauth-period`

Extra line to keep the above line from following the figure onto the next page.

Example configuration of device deployment

The switch provides simplified deployment of devices, such as access points, IP phones, security cameras, and printers, through the use of a locally configured repository that provides authentication and dynamic port assignment, such as QoS, PoE, and tagged VLANs.
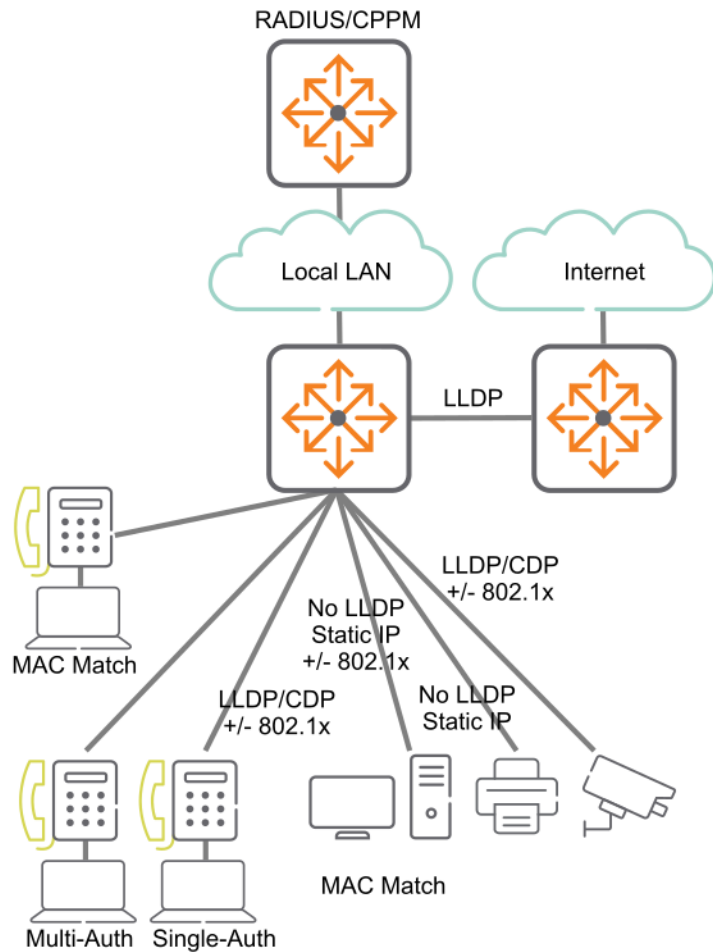
Device profiles

> Device profiles rely on role configurations. For information on role configurations, see the *Security Guide*.

Device profiles are used to dynamically assign port attributes based on the type of devices connected, without having to create a RADIUS infrastructure. You can map device profiles to device groups. A device group contains various match criteria, which can be obtained from multiple sources, such as LLDP, CDP, and local MAC match. Device profiles contain port attributes to be assigned to the port when a connected device matches a device group.

Device profiles are supported on different scenarios. It can be applied on interfaces that are configured with security (802.1X or MAC authentication), or applied based on L2 port (LLDP, CDP), or applied on standalone ports with the block-until-profile-applied command enabled. All the methods are mutually exclusive of each other. The block-until-profile-applied mode must be configured only when there is a standalone port where no security has been configured and when you want the port to be offline until at least one client is onboarded based on the match and ignore criteria that you configure. Local MAC match is supported when you configure block-until-profile-applied command or device profile with security.

> Up to 16 device profiles can be configured on the 6400.

See the *Security Guide* for the following commands:

- The `port-access onboarding-method precedence` command—If you are configuring both security and device profile on the port, and you want to configure the order in which the methods will be executed.
- The `port-access fallback-role` command—If you want to configure a role that must be applied to devices when no other role exists or can be derived for that device.

If you configure a match criteria that matches across multiple device profiles, then the priority considered is LLDP, CDP, and then local MAC match. That is, LLDP precedes over CDP, which in turn precedes over local MAC match.

The following figure displays a simple configuration of device profile and AAA authentication with RADIUS server and Aruba ClearPass Policy Manager. Local MAC match feature is useful when you do not want to afford RADIUS infrastructure or when you want to use local authentication as a backup method in case the RADIUS server is unreachable.

Figure 6 *Example of device profile setup along with RADIUS infrastructure*

;" />
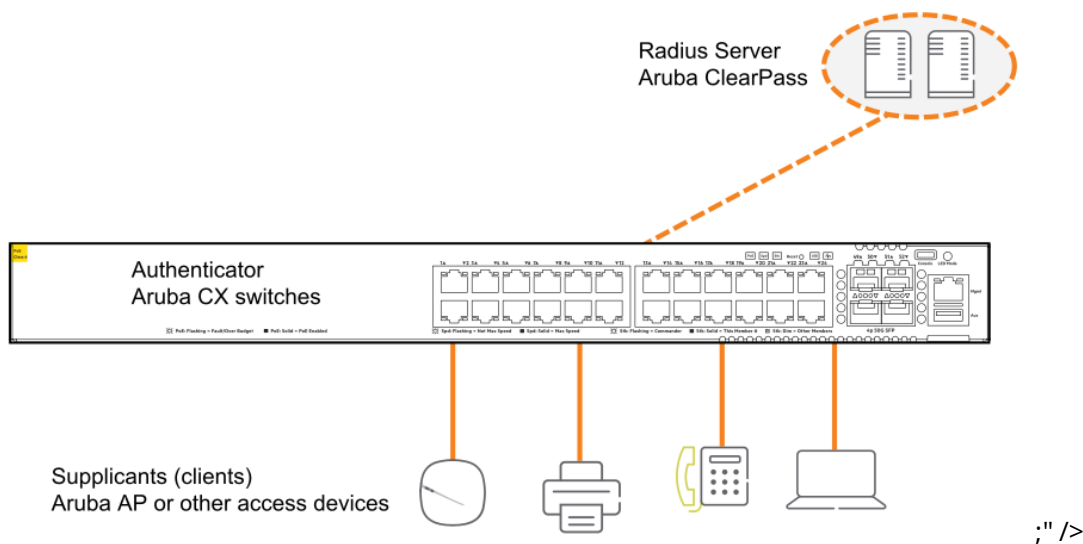
Configuring a device profile for LLDP

Procedure

1. Create an LLDP group with the command `port-access lldp-group`.
2. Define rules for adding devices to an LLDP group with the command `match`.
3. Define rules for ignoring devices so that they are not added to an LLDP group with the command `ignore`.
4. Create a device profile with the command `port-access device-profile`.
5. Add the LLDP group with the command `associate lldp-group`.
6. Add a role to a device profile with the command `associate role`. Make sure that the role is already created. For information on how to create a role, see port access role information in the *Security Guide*.
7. Enable the device profile with the command `enable`.

Configuring a device profile for CDP

1. Create a CDP group with the command `port-access cdp-group`.
2. Define rules for adding devices to a CDP group with the command `match`.

3. Define rules for ignoring devices so that they are not added to a CDP group with the command `ignore`.

4. Create a device profile with the command `port-access device-profile`.

5. Add a CDP group to a device profile with the command `associate cdp-group`.

6. Add a role to a device profile with the command `associate role`. Make sure that the role is already created. For information on how to create a role, see port access role information in the *Security Guide*.

7. Enable a device profile with the command `enable`.

Configuring a device profile for local MAC match

Procedure

1. Create a MAC group with the `mac-group` command.

2. Define rules for adding devices to a MAC group with the `match (for MAC groups)` command.

3. Define rules for ignoring devices so that they are not added to a MAC group with the `ignore (for MAC groups)` command.

4. Create a device profile with the `port-access device-profile` command.

5. Associate a MAC group with a device profile with the `associate mac-group` command.

6. Add a role to a device profile with the `associate role` command. Make sure that the role is already created. For information on how to create a role, see port access role information in the *Security Guide*.

7. Enable a device profile with the `enable` command.

Device profile commands

aaa authentication port-access allow-cdp-bpdu

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

Description

Allows all packets related to the CDP (Cisco Discovery Protocol) BPDU (Bridge Protocol Data Unit) on a secure port.

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

Examples

On the 6400 Switch Series, interface identification differs.

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

```
switch(config)# interface 1/1/1
switch(config-if)# aaa authentication port-access allow-cdp-bpdu
switch(config-if)# do show running-config
Current configuration:
!
!Version AOS-CX 10.0X.0000
led locator on
!
!
```

```
vlan 1
aaa authentication port-access mac-auth
    enable
aaa authentication port-access dot1x authenticator
    enable
interface 1/1/1
    no shutdown
    vlan access 1
    aaa authentication port-access allow-cdp-bpdu
    aaa authentication port-access mac-auth
        enable
    aaa authentication port-access dot1x authenticator
    enable

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-if`	Administrators or local user group members with execution rights for this command.

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

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

Description

Allows a client to be logged off from the system via a special TLV in the CDP packet. By default, proxy logoff via CDP packet support is disabled. When `allow-cdp-proxy-logoff` is enabled, TLV received from CDP packets corresponding to logoff processing will be read and logoff is issued to the clients. This only works on client authentication enabled ports and `aaa authentication port-access allow-cdp-bpdu` must be enabled to process .

Examples

On the 6400 Switch Series, interface identification differs.

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

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

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

Command History

Release	Modification
10.09.1000	Command introduced.

Command Information

Platforms	Command context	Authority
6300 6400	`config-if`	Administrators or local user group members with execution rights for this command.

aaa authentication port-access allow-lldp-bpdu

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

Description

Allows all packets related to the LLDP BPDU (Bridge Protocol Data Unit) on a secure port.

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

Examples

On the 6400 Switch Series, interface identification differs.

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-if`	Administrators or local user group members with execution rights for this command.

associate cdp-group

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

Description

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

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

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

Examples

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-device-profile`	Administrators or local user group members with execution rights for this command.

associate lldp-group

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

Description

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

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

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

Examples

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-device-profile`	Administrators or local user group members with execution rights for this command.

associate mac-group

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

Description

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

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

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

Examples

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-device-profile`	Administrators or local user group members with execution rights for this command.

associate role

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

Description

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

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

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

Examples

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-device-profile`	Administrators or local user group members with execution rights for this command.

disable

```
disable
no disable
```

Description

Disables a device profile.

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

Examples

Disabling a device profile:

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

Enabling a device profile named profile01:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-device-profile`	Administrators or local user group members with execution rights for this command.

enable

```
enable
no enable
```

Description

Enables a device profile.

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

Examples

Enabling a device profile:

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

Disabling a device profile named profile01:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-device-profile`	Administrators or local user group members with execution rights for this command.

ignore (for CDP groups)

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

Description

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

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

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

Examples

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

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-cdp-group`	Administrators or local user group members with execution rights for this command.

ignore (for LLDP groups)

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

Description

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

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

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

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

Examples

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-lldp-group`	Administrators or local user group members with execution rights for this command.

ignore (for MAC groups)

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

Description

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

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

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

Usage

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

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

Examples

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

```
switch(config)# mac-group grp01
switch(config-mac-group)# ignore mac 1a:2b:3c:4d:5e:6f
switch(config-mac-group)# match mac-oui 1a:2b:3c
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
!
!
ssh server vrf mgmtdefault
!
!
!
!
!
vlan 1
interface mgmt
    no shutdown
    ip dhcp
mac-group grp01
    seq 10 ignore mac 1a:2b:3c:4d:5e:6f
    seq 20 match mac-oui 1a:2b:3c
```

```
```
```

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

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

```
```

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

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

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

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

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

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

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

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

```
```

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

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

```
```

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

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 ignore mac b2:c3:44:12:78:11
switch(config-mac-group)# seq 20 ignore mac-oui 1a:2b:3c
switch(config-mac-group)# seq 30 ignore mac-mask 71:14:89:f3/32
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
vlan 1
interface mgmt
```

```
    no shutdown
    ip dhcp
mac-group grp01
    seq 10 ignore mac b2:c3:44:12:78:11
    seq 20 ignore mac-oui 1a:2b:3c
    seq 30 ignore mac-mask 71:14:89:f3/32

```

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

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

```

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	config-mac-group	Administrators or local user group members with execution rights for this command.

mac-group

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

Description

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

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

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

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

Examples

Creating a MAC group named `grp01`:

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

Removing a MAC group named `grp01`:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

match (for CDP groups)

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

Description

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

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

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

Examples

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

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

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-cdp-group`	Administrators or local user group members with execution rights for this command.

match (for LLDP groups)

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

Description

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

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

Parameter	Description
`seq <SEQ-ID>`	Specifies the ID of the rule to create or modify. If no ID is specified when adding a rule, an ID is automatically assigned in increments of 10 in the order in which rules are added. When more than one rule matches the command entered, the rule with the lowest ID takes precedence.
`sys-desc <SYS-DESC>`	Specifies the LLDP system description type-length-value (TLV). Range: 1 to 256 alphanumeric characters.
`sysname <SYS-NAME>`	Specifies the LLDP system name TLV. Range: 1 to 64 alphanumeric characters.
`vendor-oui <VENDOR-OUI>`	Specifies the LLDP system vendor OUI TLV. Range: 1 to 6 alphanumeric characters.
`type <KEY>`	Specifies the vendor OUI subtype key.
`value  <VALUE>`	Specifies the vendor OUI subtype value. Range: 1 to 256 alphanumeric characters.

Examples

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

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

Current configuration:
```

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

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

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

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

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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-lldp-group`	Administrators or local user group members with execution rights for this command.

match (for MAC groups)

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

Description

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

You must not configure the following special MAC addresses:

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

```
```

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

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

```
```

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

```
switch(config)# mac-group grp01
switch(config-mac-group)# seq 10 match mac b2:c3:44:12:78:11
switch(config-mac-group)# seq 20 match mac-oui 1a:2b:3c
switch(config-mac-group)# seq 30 match mac-mask 71:14:89:f3/32
switch(config-mac-group)# exit
switch(config)# do show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.0X.0001
!export-password: default
led locator on
!
!
```

```
vlan 1
interface mgmt
    no shutdown
    ip dhcp
mac-group grp01
    seq 10 match mac b2:c3:44:12:78:11
    seq 20 match mac-oui 1a:2b:3c
    seq 30 match mac-mask 71:14:89:f3/32

```
```

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

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

```
```

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

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

```
```

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

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


```
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-mac-group`	Administrators or local user group members with execution rights for this command.

port-access cdp-group

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

Description

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

The no form of this command removes a CDP group.

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

Examples

Creating a CDP group named grp01:

```
switch(config)# port-access cdp-group grp01
switch(config-cdp-group)# match platform CISCO
```

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

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

Removing a CDP group named grp01:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	config	Administrators or local user group members with execution rights for this command.

port-access device-profile

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

Description

Creates a new device profile and switches to the `config-device-profile` context. A maximum of 32 device profiles can be created.

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

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

Examples

Creating a device profile named **profile01**:

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

Removing a device profile named **profile01**:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

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

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

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

Description

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

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

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

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

Example

On the 6400 Switch Series, interface identification differs.

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-if` `config-if-deviceprofile`	Administrators or local user group members with execution rights for this command.

port-access lldp-group

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

Description

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

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

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

Examples

Creating an LLDP group named grp01:

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

Removing an LLDP group named grp01:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config`	Administrators or local user group members with execution rights for this command.

show port-access device-profile

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

Description

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

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

Examples

On the 6400 Switch Series, interface identification differs.

Showing the applied state of the device profiles:

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

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

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

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

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

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

```
switch# show port-access device-profile interface 1/1/3 client-status
00:0c:29:9e:d1:20

Port 1/1/3, Neighbor-Mac  00:0c:29:9e:d1:20
    Profile Name    : lobbyaps
    LLDP Group      :
    CDP Group       : aruba-ap_cdp
    MAC Group       :
    Role            : test_ap_role
    Status          : Failed
    Failure Reason  : Failed to apply MAC based VLAN
```

Showing the applied state of a specific device profile:

```
switch# show port-access device-profile name lldp-group

    Profile Name            : lldp-group
    LLDP Groups             :
    CDP Groups              :
    MAC Groups              : pc-behind-phone, lldp
    Role                    : auth_role
    State                   : Enabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Manager (#)	Administrators or local user group members with execution rights for this command.

LLDP

The IEEE 802.1AB Link Layer Discovery Protocol (LLDP) provides a standards-based method for network devices to discover each other and exchange information about their capabilities. An LLDP device advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets on all interfaces on which outbound LLDP is enabled, and reading LLDP advertisements from neighbor devices on ports on which inbound LLDP is enabled. Inbound packets from neighbor devices are stored in a special LLDP MIB (management information base). This information can then be queried by other devices through SNMP.

LLDP information is used by network management tools to create accurate physical network topologies by determining which devices are neighbors and through which interfaces they connect. LLDP operates at layer 2 and requires an LLDP agent to be active on each interface that sends and receives LLDP advertisements. LLDP advertisements can contain a variable number of TLV (type, length, value) information elements. Each TLV describes a single attribute of a device such as: system capabilities, management IP address, device ID, port ID.

Packet boundaries

When multiple LLDP devices are directly connected, an outbound LLDP packet travels only to the next LLDP device. An LLDP-capable device does not forward LLDP packets to any other devices, regardless of whether they are LLDP-enabled.

An intervening hub or repeater forwards the LLDP packets it receives in the same manner as any other multicast packets it receives. Therefore, two LLDP switches joined by a hub or repeater handle LLDP traffic in the same way that they would if directly connected.

Any intervening 802.1D device or Layer-3 device that is either LLDP-unaware or has disabled LLDP operation drops the packet.

LLDP-MED

LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. LLDP-MED in the switches uses the standard LLDP commands described earlier in this section, with some extensions, and also introduces new commands unique to LLDP-MED operation. The show commands described elsewhere in this section are applicable to both LLDP and LLDP-MED operation. LLDP-MED enables:

- Configure Voice VLAN and advertise it to connected MED endpoint devices.
- Power over Ethernet (PoE) status and troubleshooting support via SNMP.

LLDP agent

When you enable LLDP on the switch, it is automatically enabled on all data plane interfaces. You can customize this behavior by manually enabling/disabling support on each interface.

Supported standards

The LLDP agent supports the following standards: IEEE 802.1AB-2005, Station, and Media Access Control Connectivity Discovery.

Supported interfaces

LLDP is supported on interfaces mapped to a physical port, and the Out-Of-Band Management (OOBM) port. It is not supported on logical interfaces, such as loopback, tunnels, and SVIs.

Operating modes

When LLDP is enabled, the switch periodically transmits an LLDP advertisement (packet) out each active port enabled for outbound LLDP transmissions and receives LLDP advertisements on each active port enabled to receive LLDP traffic.

The LLDP agent can operate in one of the following modes:

- Transmit and receive (TxRx): This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets and to store the data from received (inbound) LLDP packets in the switch's MIB.
- Transmit only (Tx): Enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.
- Receive only (Rx): Enables a port to receive and read LLDP packets from LLDP neighbors and to store the packet data in the switch's MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.

- Disabled: Disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.

An LLDP agent operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes.

Sending LLDP frames

Each time the LLDP operating mode of an LLDP agent changes, its LLDP protocol state machine reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, an LLDP agent must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.

Receiving LLDP frames

An LLDP agent operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the LLDP agent saves the information and starts an aging timer. The initial value of the aging timer is equal to the TTL value in the Time To Live TLV carried in the LLDP frame. When the LLDP agent receives a new LLDP frame, the aging timer restarts. When the aging timer decreases to zero, all saved information ages out.

TLV support

By default, the agent sends and receives the following mandatory TLVs on each interface:

- Port ID
- Chassis ID
- TTL

By default, the following ANSI/TIA-1057 TLVs for LLDP Media Endpoint Discovery (MED) are enabled on an agent. Sending them depends on the configuration and reception of any MED TLVs:

- MAC/PHY status. Includes the bit rate and auto negotiation status of the link.
- Power Via MDI: Includes Power Over Ethernet related information for supported interfaces.
- Port description
- System name
- System description
- Management address
- System capabilities
- Port VLAN ID

By default, the agent sends and receives the following ANSI/TIA-1057 TLVs for LLDP Media Endpoint Discovery (MED):

- Capabilities: Indicates MED TLV capability.
- Power Via MDI: Includes Power Over Ethernet related information.
- Network Policy: Includes the VLAN configuration for voice application.
- Location: Location identification information.
- Extended Power Via MDI: Power Over Ethernet related information

TLV advertisements

The LLDP agent transmits the following:

- Chassis-ID: Base MAC address of the switch.
- Port-ID: Port number of the physical port.
- Time-to-Live (TTL): Length of time an LLDP neighbor retains advertised data before discarding it.
- System capabilities: Identifies the primary switch capabilities (bridge, router). Identifies the primary switch functions that are enabled, such as routing.
- System description: Includes switch model name and running software version, and ROM version.
- System name: Name assigned to the switch.
- Management address: Default address selection method unless an optional address is configured.
- Port description: Physical port identifier.
- Port VLAN ID: On an L2 port, contains access or native VLAN ID. On an L3 port, contains a value of 0. Trunk allowed VLANs information are not advertised as part of the Port VLAN ID TLV. (Not supported on the OOBM interface)

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

On the 6400 Switch Series, interface identification differs.

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 eee

```
lldp dot3 eee
no lldp dot3 eee
```

Description

Sets the 802.3 TLVs for Energy-Efficient Ethernet (EEE) to be advertised. By default, advertisement of EEE TLVs is enabled. Not supported on the OOBM interface.

The `no` form of this command disables advertisement of 802.3 TLVs.

Parameter	Description
`eee`	Specifies advertisement of 802.3 TLVs for EEE.

Examples

Enabling advertisement of the EEE TLVs:

```
switch(config-if)# lldp dot3 eee
```

Disabling advertisement of the EEE TLVs:

```
switch(config-if)# no lldp dot3 eee
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	`config-if`	Administrators or local user group members with execution rights for this command.

lldp holdtime

```
lldp holdtime <TIME>
```

```
no lldp holdtime
```

Description

Sets the holdtime 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 to its default value of 4.

Parameter	Description
`<TIME>`	Specifies the holdtime in seconds. Range: 2 to 10. Default: 4.

Examples

Setting the holdtime to 8 seconds:

```
switch(config)# lldp holdtime 8
```

Setting the holdtime to the default value of 4 seconds:

```
switch(config)# no lldp holdtime
```

Command History

Release	Modification
10.07 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-ipv4-address

```
lldp management-ipv4-address <IPV4-ADDR>
no lldp management-ipv4-address
```

Description

Defines the IPv4 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-ipv4-address 10.10.10.2
```

Removing the management address:

```
switch(config)# no lldp management-ipv4-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 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.

Examples

Enabling support for the LLDP MED emergency location TLV:

```
switch(config-if)# lldp med-location elin-addr gher
```

Disabling support for the LLDP MED emergency location TLV:

```
switch(config-if)# no lldp med-location elin-addr gher
```

Enabling support for the LLDP MED civic address TLV:

```
switch(config-if)# lldp med-location civic-addr US 1 4 ret 6 tyu 7 tiyuo
```

Disabling support for the LLDP MED civic address TLV:

```
switch(config-if)# no lldp med-location civic-addr US 1 4 ret 6 tyu 7 tiyuo
```

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

On the 6400 Switch Series, interface identification differs.

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.

Parameter	Description

`select-tlv <TLV-NAME>`	Specifies the TLV name to send. The following TLV names are supported:
	
	■ `management-address`: Selected as follows:
	  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`: A description of the port.
	■ `port-vlan-id`: VLAN ID assigned to the port.
	■ `system-capabilities`: Identifies the primary switch functions that are enabled, such as routing.
	■ `system-description`: Description of the system, comprised of the following information: hardware serial number, hardware revision number, and firmware version.
	■ `system-name`: Host name assigned to the switch.

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 port-description
```

Command History

Release	Modification
10.07 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 transmit

```
lldp transssmit
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

On the 6400 Switch Series, interface identification differs.

Enabling LLDP transmission on interface **1/1/1**:

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

Disabling LLDP transmission on interface **1/1/1**:

```
switch(config)# interface 1/1/1
switch(config-if)# no lldp transssmit
```

Enabling LLDP transmission on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# lldp transsmit
```

Disabling LLDP transmission on the OOBM interface:

```
switch(config)# interface mgmt
switch(config-if)# no lldp transsmit
```

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

On the 6400 Switch Series, interface identification differs.

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
=======================
PORT          TX-ENABLED        RX-ENABLED        INTF-TRAP-ENABLED
--------------------------------------------------------------------------
1/1/1         Yes               Yes               Yes
```

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 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
6300 6400	Manager (#)	Operators 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   : Aruba 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   : Aruba
Management Address   : 192.168.10.1
Capabilities Available : Bridge, Router
Capabilities Enabled   : Bridge, Router
TTL                  : 120

Port Based Data
===============

Port-ID           : 1/1/11
Port-Desc         : "1/1/11"
Port Mgmt-Address : 164.254.21.220
Port VLAN ID      : 0

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  : Aruba
Management Address   : 192.168.10.1
Capabilities Available : Bridge, Router
Capabilities Enabled   : Bridge, Router
TTL                 : 120

Port Based Data
===============

Port-ID             : 1/1/11
Port-Desc           : "1/1/11"
Port VLAN ID        : 100
Parent Interface    : interface 1/1/11
```

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

On the 6400 Switch Series, interface identification differs.

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         :
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 Aruba IAP
Neighbor Chassis-ID           : 84:d4:7e:ce:5d:68
Neighbor Management-Address   : 169.254.41.250
Chassis Capabilities Available : Bridge, WLAN
Chassis Capabilities Enabled  : WLAN
Neighbor Port-ID              : 84:d4:7e:ce:5d:68
Neighbor Port-Desc            : eth0
TTL                           : 120
Neighbor Port VLAN ID         :
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 : Aruba 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       :
TTL                         : 120
Neighbor Chassis-Name       : switch
Neighbor Chassis-Description : Aruba 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       :
TTL                         : 120
Neighbor Chassis-Name       : switch
Neighbor Chassis-Description : Aruba 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
TTL                         : 120
Neighbor Chassis-Name       : switch
Neighbor Chassis-Description : Aruba 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
TTL                         : 120
```

Showing neighbor information for interface 1/3/2 when it has EEE enabled and successfully auto-negotiated:

```
switch# show lldp neighbor-info 1/3/2

Port                          : 1/3/2
Neighbor Entries              : 1
Neighbor Entries Deleted      : 1
Neighbor Entries Dropped      : 0
Neighbor Entries Aged-Out     : 1
Neighbor Chassis-Name         : BLDG01-F1-6300
Neighbor Chassis-Description  : Aruba JL668A  FL.10.07.0001BN
Neighbor Chassis-ID           : 88:3a:30:92:a5:c0
Neighbor Management-Address   : 10.6.9.15
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID              : 1/1/1
Neighbor Port-Desc            : 1/1/1
Neighbor Port VLAN ID         : 1
TTL                           : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported   : true
Neighbor Auto-Neg Enabled     : true
Neighbor Auto-Neg Advertised  : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type             : 1000 BASETFD

Neighbor EEE information       : DOT3
Neighbor TX Wake time         : 17 us
Neighbor RX Wake time         : 17 us
Neighbor Fallback time        : 17 us
Neighbor TX Echo time         : 17 us
Neighbor RX Echo time         : 17 us
```

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

On the 6400 Switch Series, interface identification differs.

Showing detailed LLDP information for all interfaces:

```
switch# show lldp neighbor-info detail

LLDP Neighbor Information
=========================

Total Neighbor Entries         : 6
Total Neighbor Entries Deleted  : 2
Total Neighbor Entries Dropped  : 0
Total Neighbor Entries Aged-Out : 2


--------------------------------------------------------------------------

Port                          : 1/1/1
Neighbor Entries              : 1
Neighbor Entries Deleted      : 0
Neighbor Entries Dropped      : 0
Neighbor Entries Aged-Out     : 0
Neighbor Chassis-Name         : 6300
Neighbor Chassis-Description  : Aruba ...
Neighbor Chassis-ID           : 38:11:17:1a:d5:00
Neighbor Management-Address   : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled  : Bridge, Router
Neighbor Port-ID              : 1/1/4
Neighbor Port-Desc            : 1/1/4
Neighbor Port VLAN ID         : 1
TTL                           : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported   : true
Neighbor Auto-Neg Enabled     : true
Neighbor Auto-Neg Advertised  : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type             : 1000 BASETFD


--------------------------------------------------------------------------

Port                          : 1/1/2
Neighbor Entries              : 1
Neighbor Entries Deleted      : 0
Neighbor Entries Dropped      : 0
Neighbor Entries Aged-Out     : 0
Neighbor Chassis-Name         : 6300
Neighbor Chassis-Description  : Aruba ...
Neighbor Chassis-ID           : 38:11:17:1a:d5:00
Neighbor Management-Address   : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled  : Bridge, Router
Neighbor Port-ID              : 1/1/5
Neighbor Port-Desc            : 1/1/5
Neighbor Port VLAN ID         : 1
TTL                           : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported   : true
Neighbor Auto-Neg Enabled     : true
Neighbor Auto-Neg Advertised  : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type             : 1000 BASETFD
```

```
--------------------------------------------------------------------------------
Port                        : 1/1/3
Neighbor Entries            : 1
Neighbor Entries Deleted    : 0
Neighbor Entries Dropped    : 0
Neighbor Entries Aged-Out   : 0
Neighbor Chassis-Name       : 6300
Neighbor Chassis-Description : Aruba ...
Neighbor Chassis-ID         : 38:11:17:1a:d5:00
Neighbor Management-Address  : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID            : 1/1/6
Neighbor Port-Desc          : 1/1/6
Neighbor Port VLAN ID       : 1
TTL                         : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported   : true
Neighbor Auto-Neg Enabled     : true
Neighbor Auto-Neg Advertised  : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type             : 1000 BASETFD

--------------------------------------------------------------------------------
Port                        : 1/1/46
Neighbor Entries            : 1
Neighbor Entries Deleted    : 0
Neighbor Entries Dropped    : 0
Neighbor Entries Aged-Out   : 0
Neighbor Chassis-Name       : 6300
Neighbor Chassis-Description : Aruba ...
Neighbor Chassis-ID         : 38:11:17:1a:d5:00
Neighbor Management-Address  : 38:11:17:1a:d5:00
Chassis Capabilities Available : Bridge, Router
Chassis Capabilities Enabled   : Bridge, Router
Neighbor Port-ID            : 1/1/19
Neighbor Port-Desc          : 1/1/19
Neighbor Port VLAN ID       : 1
TTL                         : 120

Neighbor Mac-Phy details
Neighbor Auto-neg Supported   : true
Neighbor Auto-Neg Enabled     : true
Neighbor Auto-Neg Advertised  : 1000 BASE_TFD, 100 BASE_T4, 10 BASET_FD
Neighbor MAU type             : 1000 BASETFD

--------------------------------------------------------------------------------
Port                        : 1/1/47
Neighbor Entries            : 1
Neighbor Entries Deleted    : 0
Neighbor Entries Dropped    : 0
Neighbor Entries Aged-Out   : 0
Neighbor Chassis-Name       : 6300
Neighbor Chassis-Description : Aruba ...
Neighbor Chassis-ID         : 38:11:17:1a:d5:00
Neighbor Management-Address  : 38:11:17:1a:d5:00
Chassis Cap
```

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
Neighbor Port VLAN ID       :
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 : Aruba 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        :
TTL                          : 120

Neighbor Chassis-Name        : switch
Neighbor Chassis-Description : Aruba 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        :
TTL                          : 120

Neighbor Chassis-Name        : switch
Neighbor Chassis-Description : Aruba 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        :
TTL                          : 120

Neighbor Chassis-Name        : switch
Neighbor Chassis-Description : Aruba 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        :
TTL                          : 120
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Manager (#)	Operators 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

On the 6400 Switch Series, interface identification differs.

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
6300 6400	Manager (#)	Operators 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
```

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 1/1/1
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

On the 6400 Switch Series, interface identification differs.

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

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

On the 6400 Switch Series, interface identification differs.

Showing all CDP neighbor information:

```
switch(config)# show cdp neighbor-info
Port         Device ID                 Platform                      Capability
-------------------------------------------------------------------------------
1/1/1        myswitch                  cisco WS-C2950-12         SI
```

Showing CDP information for interface **1/1/1**:

```
switch(config)# show cdp neighbor-info 1/1/1
Local Port : 1/1/1
MAC                : 3c:a8:2a:7b:6b:2b
Device ID          : SEPd4adbd2a30d6
Address            : 2.71.0.230
Platform           : Cisco IP Phone 3905
Duplex             : full
Capability         : host
Voice VLAN Support : Yes
Neighbor Port-ID   : Port 1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show cdp traffic

```
show cdp neighbor-info
```

Description

Shows CDP statistics for each interface.

Examples

On the 6400 Switch Series, interface identification differs.

Showing CDP traffic statistics:

```
switch(config)# show cdp traffic
CDP Statistics
===================
Port          Transmitted Frames      Received Frames        Discarded Frames
--------------------------------------------------------------------------------
1/1/1            0                        4                        0
1/1/2            0                        0                        0
1/1/3            0                        2                        0
1/1/4            0                        0                        0
1/1/5            0                        0                        0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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 support

The switch supports standards-based Zero Touch Provisioning (ZTP) operations as follows:

- The switch must be running the factory default configuration.
- The switch can connect to the DHCP server from the OOBM management port.

  The switch can connect to the DHCP server from either the OOBM management port, or a data port on the default VLAN.

- ZTP operations are supported over IPv4 connections only. IPv6 connections are not supported for ZTP operations.
- 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 DHCP options 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

DHCP option	Description
43 suboption 148	FQDN or IPv4 address of the HTTP Proxy
60	Vendor Class Identifier (VCI)
66	IPv4 address of the TFTP 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.)

- 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.

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."

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 server and record its IP address. The address is required when you set up the DHCP server. The switch must be able to reach the TFTP server and DHCP server, either on the same subnet, or on a remote subnet via DHCP relay.

   Switches support provisioning through a network connected to a data port or through a network connected to the management port.

3. Publish the configuration files and image files to the TFTP server. You need to know the locations of the files and the IP address of the TFTP 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 IP address of the TFTP server. Using a host name is not supported.
   - The path to the switch configuration and firmware image files on the TFTP 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 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 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.

   On switches that support ZTP operations on data ports, the switch also sends out a DHCP discovery from all data ports in the default VLAN.

   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.

   On switches that support ZTP operations on data ports, DHCP options received on the management port have priority over DHCP options received on data ports:
   - If DHCP options are received on the management port before being received on a data port, the switch processes those options immediately.
   - If DHCP options are received on a data port, the switch waits an additional 30 seconds for options to be received on the management port. If no DHCP options are received on the management port during those 30 seconds, the switch processes the DHCP options it received on the data port.

   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 address of the TFTP 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 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 IP address of the TFTP server
- The name of the image file
- The name of the configuration file

The `show ztp information` command shows the options offered by the DHCP server and the status of the ZTP operation.

The status of the ZTP operation is one of the following:

Success

The ZTP operation succeeded.

One of the following is true:

- Both the running configuration and the startup configuration were updated.
- The IP address of the TFTP server was received, but the offer did not include a configuration file or a firmware image file.
- Any combination of vendor encapsulated DHCP options are received as configured, along with the firmware image and switch configuration file.
- Only vendor encapsulated DHCP options are configured and are received accordingly.

Failed - Custom startup configuration detected

The switch was booted from a configuration that is not the factory default configuration. For example, the administrator password has been set.

Failed - Timed out while waiting to receive ZTP options

Either the switch received the DHCP IPv4 address but no ZTP options were received within 1 minute or ZTP force-provision is triggered and no ZTP options are received within 3 minutes.

Failed - Detected change in running configuration

The running configuration was modified by a user while the ZTP operation was in progress.

Failed - TFTP server unreachable

The TFTP server is not reachable at the specified IP address.

Failed - TFTP server information unavailable

The image file name or config file name is provided without the TFTP server location to fetch the files from and ZTP enters failed state.

Failed - Invalid configuration file received

Either the file transfer of the configuration file failed, or the configuration file is invalid (an error occurred while attempting to apply the configuration).

Failed - Invalid image file received

Either the file transfer of the firmware image file failed, or the firmware image file is invalid (an error occurred while verifying the image).

Examples

Showing switch image download in progress after receiving ZTP options:

```
switch# show ztp information
TFTP Server                 : 10.0.0.2
Image File                  : TL_10_02_0001.swi
Configuration File          : config_file
ZTP Status                  : In-progress - Image download and verification
Aruba Central Location      : secure.arubanetworks.com
Aruba Central Shared Token  : aruba123
Force-Provision             : Disabled
HTTP Proxy Location         : http.proxy.arubanetworks.com
```

Showing switch image download failure after receiving ZTP options:

```
switch# show ztp information
TFTP Server                 : 10.0.0.2
Image File                  : TL_10_02_0001.swi
Configuration File          : config_file
ZTP Status                  : Failed - Unable to download image
Aruba Central Location      : secure.arubanetworks.com
Aruba Central Shared Token  : aruba123
Force-Provision             : Disabled
HTTP Proxy Location         : http.proxy.arubanetworks.com
```

Showing switch configuration download in progress after receiving ZTP options:

```
switch# show ztp information
TFTP Server                 : 10.0.0.2
Image File                  : TL_10_02_0001.swi
Configuration File          : config_file
ZTP Status                  : In-progress - Configuration download
Aruba Central Location      : secure.arubanetworks.com
Aruba Central Shared Token  : aruba123
Force-Provision             : Disabled
HTTP Proxy Location         : http.proxy.arubanetworks.com
```

Showing switch configuration download failure after receiving ZTP options:

```
switch# show ztp information
TFTP Server                 : 10.0.0.2
Image File                  : TL_10_02_0001.swi
Configuration File          : config_file
ZTP Status                  : Failed - Unable to download configuration
Aruba Central Location      : secure.arubanetworks.com
Aruba Central Shared Token  : aruba123
Force-Provision             : Disabled
HTTP Proxy Location         : http.proxy.arubanetworks.com
```

Showing switch failure to update start-up confriguration after downloading configuration received from ZTP options:

```
switch# show ztp information
TFTP Server                 : 10.0.0.2
```

```
Image File                     : TL_10_02_0001.swi
Configuration File             : config_file
ZTP Status                     : Failed - Could not copy to start-up configuration
Aruba Central Location         : secure.arubanetworks.com
Aruba Central Shared Token     : aruba123
Force-Provision                : Disabled
HTTP Proxy Location            : http.proxy.arubanetworks.com
```

In the following example, the ZTP operation succeeded, and both an image file and a configuration file were provided.

```
VSF-10-Mbr# show ztp information
TFTP Server                    : 10.1.84.160
Image File                     : FL_10_06_0001CK.swi
Configuration File             : 102720-new-setup-config-updated.txt
Status                         : Success
Aruba Central Location         : NA
Aruba Central Shared Token     : aruba123
Force-Provision                : Disabled
HTTP Proxy Location            : NA
VSF-10-Mbr#
```

In the following example, the ZTP option succeeded. A configuration file was not provided, but an image file was provided.

```
VSF-10-Mbr# show ztp information
TFTP Server                    : 10.1.84.160
Image File                     : TL_10_02_0001.swi
Configuration File             : NA
Status                         : Success
Aruba Central Location         : NA
Aruba Central Shared Token     : aruba123
Force-Provision                : Disabled
HTTP Proxy Location            : NA
VSF-10-Mbr#
```

In the following example, the ZTP operation failed because the TFTP server was unreachable.

```
VSF-10-Mbr# show ztp information
TFTP Server                    : 10.1.84.160
Image File                     : TL_10_02_0001.swi
Configuration File             : 102720-new-setup-config-updated.txt
Status                         : Failed - TFTP server unreachable
Aruba Central Location         : NA
Aruba Central Shared Token     : NA
Force-Provision                : Disabled
HTTP Proxy Location            : NA
VSF-10-Mbr#
```

In the following example, the ZTP operation was stopped because the switch did not receive any options from the DHCP server for ZTP within 1 minute of receiving the IP address from the server.

```
VSF-10-Mbr## show ztp information
TFTP Server                   : NA
Image File                    : NA
Configuration File            : NA
Status                        : Failed - Timed out while waiting to receive ZTP options
Aruba Central Location        : NA
Aruba Central Shared Token    : NA
Force-Provision               : Disabled
HTTP Proxy Location           : NA
VSF-10-Mbr#
```

In the following example, the ZTP operation was stopped because the switch was booted from a configuration that was not the factory default configuration.

```
switch# show ztp information
TFTP Server                   : 10.0.0.2
Image File                    : TL_10_02_0001.swi
Configuration File            : ztp.cfg
Status                        : Failed - Custom startup configuration detected
Aruba Central Location        : NA
Aruba 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 (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

ztp force provision

```
ztp force-provision
no ztp force-provision
```

Description

Starts on-demand ZTP.

Usage

DHCP options received are processed independent of he current state of configuration on the switch. Previous ZTP TFTP Server, Image File, Configuration File, Aruba Central Location, and HTTP Proxy location options are cleared and the switch sends a DHCP request.

Examples

In the following example, force-provision is enabled.

```
switch# configure terminal
switch(config)# ztp force-provision
```

In the following example, force-provision status is checked while enabled.

```
switch# show ztp information
TFTP Server                  : 10.0.0.2
Image File                   : TL_10_02_0001.swi
Configuration File           : ztp.cfg
Status                       : Success
Aruba Central Location       : NA
Aruba Central Shared Token   : NA
Force-Provision              : Enabled
HTTP Proxy Location          : NA
```

In the following example, force-provision is disabled.

```
switch# configure terminal
switch(config)# no ztp force-provision
```

In the following example, force-provision status is checked while disabled.

```
switch# show ztp information
TFTP Server                  : 10.0.0.2
Image File                   : TL_10_02_0001.swi
Configuration File           : ztp.cfg
Status                       : Success
Aruba Central Location       : NA
Aruba Central Shared Token   : NA
Force-Provision              : Disabled
HTTP Proxy Location          : NA
```

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.

---

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
6300 6400	`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
6300 6400	`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
6300 6400	Manager (#)	Administrators or local user group members with execution rights for this command.

console baud-rate

```
console baud-rate <SPEED>
no console baud-rate <SPEED>
```

Description

Sets the console serial port speed.

The no form of this command resets the console port speed to its default of 115200 bps.

Parameter	Description
<SPEED>	Selects the console port speed in bps, either `9600` or `115200`.

Usage

The speed change occurs immediately for the active console session. The console will be inaccessible until the client terminal settings are updated to match the console port speed that you set. After the command is executed you will be prompted to log in again.

Examples

Setting the console port speed to 9600 bps:

```
switch(config)# console baud-rate 9600
This command will configure the baud rate immediately for the active serial
console session. After the command is executed the user will be prompted to
re-login. The serial console will be inaccessible until the terminal client
settings are updated to match the baud rate of the switch.
Continue (y/n)? y
```

Resetting the console port to its default speed 115200 bps:

```
switch(config)# no console baud-rate
```

Command History

Release	Modification
10.08	Command introduced

Command Information

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

domain-name

```
domain-name <NAME>
no domain-name [<NAME>]
```

Description

Specifies the domain name of the switch.

The `no` form of this command sets the domain name to the default, which is no domain name.

Parameter	Description
`<NAME>`	Specifies the domain name to be assigned to the switch. The first character of the name must be a letter or a number. Length: 1 to 32 characters.

Examples

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Setting the domain name to the default value:

```
switch(config)# no domain-name
switch(config)# show domain-name

switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

hostname

```
hostname <HOSTNAME>
no hostname [<HOSTNAME>]
```

Description

Sets the host name of the switch.

The `no` form of this command sets the host name to the default value, which is `switch`.

Parameter	Description
`<HOSTNAME>`	Specifies the host name. The first character of the host name must be a letter or a number. Length: 1 to 32 characters. Default: `switch`

Examples

Setting and showing the host name:

```
switch# show hostname
switch
switch# config
switch(config)# hostname myswitch
myswitch(config)# show hostname
myswitch
```

Setting the host name to the default value:

```
myswitch(config)# no hostname
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

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`
`admin-state {diagnostic	down	up}`	Selects the administrative state in which to put the specified module:
`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
6400	`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.
```

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
6400	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
IPV4-SRC-ADDR	Specifies the source IPv4 address to trace.

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

Examples

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

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

Type escape sequence to abort.
Mtrace from 10.0.0.1 for Source 20.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0  10.0.0.1
-1  30.0.0.1 PIM  0 ms
-2  40.0.0.1 PIM  2 ms
-3  50.0.0.1 PIM  100 ms
-4  60.0.0.1 PIM  156 ms
-5  20.0.0.1 PIM  123 ms
```

Tracing with source and group addresses:

```
(switch)# mtrace 200.0.0.1 239.1.1.1

Type escape sequence to abort.
Mtrace from self for Source 200.0.0.1 via Group 239.1.1.1
From destination(?) to source (?)...
Querying ful reverse path...
0  10.0.0.1
-1  30.0.0.1 PIM  0 ms
-2  40.0.0.1 PIM  2 ms
-3  50.0.0.1 PIM  100 ms
-4  60.0.0.1 PIM  156 ms
-5  200.0.0.1 PIM  123 ms
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Manager (#)	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>-<NNNNNNNNNN>
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
6300 6400	Operator (>) or Manager (#)	Operators 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]
```

Description

Shows boot information. When no parameters are specified, shows the most recent information about the boot operation, and the three previous boot operations for the active management module. When the `all` parameter is specified, shows the boot information for the active management module and all available line modules. To view boot-history on the standby, the command must be sent on the standby console.

Parameter	Description
`all`	Shows boot information for the active management module and all available line modules.

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.
`Index`
The position of the boot in the history file. Range: 0 to3.
`Boot ID`
A unique ID for the boot . A system-generated 128-bit string.

`Current Boot, up for <SECONDS> seconds`
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.
`Reboot requested through database`

The reboot occurred because of a request made through the CLI or other API.
`Uncontrolled reboot`
The reason for the reboot is not known.

Examples

Showing the boot history of the active management module:

```
switch# show boot-history
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
switch#
```

Showing the boot history of the active management module and all line modules:

```
switch# show boot-history all
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 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
===============================================================================
```

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 domain-name

```
show domain-name [vsx-peer]
```

Description

Shows the current domain name.

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

Usage

If there is no domain name configured, the CLI displays a blank line.

Example

Setting and showing the domain name:

```
switch# show domain-name

switch# config
switch(config)# domain-name example.com
switch(config)# show domain-name
example.com
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show environment fan

```
show environment fan [vsf | vsx-peer]
```

Description

Shows the status information for all fans and fan trays (if present) in the system.

Parameter	Description
vsf	Shows output from the VSF member-id on switches that support VSF.
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration 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 6300 switch series:

```
switch# show environment fanFan tray information
-----------------------------------------
----------------------------------
Name Description Status Serial Number
Fans
-----------------------------------------
----------------------------------
1/1 JL669A Aruba X751 FB Fan Tray ready
CN97KN9131 2
1/2 JL669A Aru
-----------------------------------------------------------------------------
1/1/1          N/A         N/A            slow     front-to-back   ok      5371
1/1/2          N/A         N/A            slow     front-to-back   ok      5320
1/1/3          N/A         N/A            slow     front-to-back   ok      5328
1/1/4          N/A         N/A            slow     front-to-back   ok      5256
1/2/1          N/A         N/A            slow     front-to-back   ok      5371
1/2/2          N/A         N/A            slow     front-to-back   ok      5349
1/2/3          N/A         N/A            slow     front-to-back   ok      5292
1/2/4          N/A         N/A            slow     front-to-back   ok      5349
1/3/1          N/A         N/A            slow     front-to-back   ok      5313
1/3/2          N/A         N/A            slow     front-to-back   ok      5371
1/3/3          N/A         N/A            slow     front-to-back   ok      5379
1/3/4          N/A         N/A            slow     front-to-back   ok      5379
1/4/1          N/A         N/A            slow     front-to-back   ok      5313
1/4/2          N/A         N/A            slow     front-to-back   ok      5299
1/4/3          N/A         N/A            slow     front-to-back   ok      5285
1/4/4          N/A         N/A            slow     front-to-back   ok      5371
```

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 <MEMBER-ID> [vsx-peer]
```

Description

Shows state and status information for all the configurable LEDs in the system.

Parameter	Description
<MEMBER-ID>	Shows output from the specified VSF member ID on switches that support VSF.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration 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
Mbr/Name        State      Status
------------------------------
1/locator       off        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

Not supported on the 6300 Switch Series.
```
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
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration 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:

`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 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.

Example

Showing the power consumption for an Aruba 6400 switch:

```
switch> show environment power-consumption
                                                          Power
Name    Type               Description                   Usage
-----------------------------------------------------------------
1/1     management-module   R0X31A 6400 Management Module    18 W
1/2     management-module                                    0 W
1/3     line-card-module                                     0 W
1/4     line-card-module    R0X39A 6400 48p 1GbE CL4 PoE 4SFP56 Mod  54 W
1/5     line-card-module                                     0 W
1/6     line-card-module    R0X39A 6400 48p 1GbE CL4 PoE 4SFP56 Mod  56 W
1/7     line-card-module    R0X39A 6400 48p 1GbE CL4 PoE 4SFP56 Mod  51 W
1/1     fabric-card-module  R0X24A 6405 Chassis               71 W


Module Total Power Usage                                   250 W
Chassis Total Power Usage                                   294 W

Chassis Total Power Available                             1800 W
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6400	Operator (>) or Manager (#)	Operators 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 [vsf | vsx-peer]
```

Description

Shows status information about all power supplies in the switch.

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

Usage

The following information is provided for each power supply:
`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.

Example

Showing the output when only one power supply is installed in an Aruba 6400 switch chassis:

```
switch#  show environment power-supply
         Product  Serial            PSU        Wattage
Mbr/PSU  Number   Number            Status     Maximum
---------------------------------------------------------
1/1      R0X36A   CN91KMM2H3        OK         3000
1/2      N/A      N/A               Absent     0
1/3      N/A      N/A               Absent     0
1/4      N/A      N/A               Absent     0
```

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 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
6300 6400	Operator (>) or Manager (#)	Operators 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] [vsf | 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.
vsf	Shows output from the VSF member-id on switches that support VSF
vsx-peer	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration 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:
`normal`
Sensor is within nominal temperature range.
`min`
Lowest temperature from this sensor.
`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 this sensor.

Examples

Showing current temperature information for a 6300 switch:

```
switch# show environment temperature
Temperature information
-----------------------------------------------------------------------------
                                                Current
Mbr/Slot-Sensor                Module Type      temperature  Status
-----------------------------------------------------------------------------
1/1-PHY-01-04                  line-card-module    45.00 C      normal
1/1-PHY-05-08                  line-card-module    45.00 C      normal
1/1-PHY-09-12                  line-card-module    46.00 C      normal
1/1-PHY-13-16                  line-card-module    47.00 C      normal
1/1-PHY-17-20                  line-card-module    47.00 C      normal
1/1-PHY-21-24                  line-card-module    50.00 C      normal
1/1-PHY-25-28                  line-card-module    45.00 C      normal
1/1-PHY-29-32                  line-card-module    47.00 C      normal
1/1-PHY-33-36                  line-card-module    48.00 C      normal
1/1-PHY-37-40                  line-card-module    47.00 C      normal
1/1-PHY-41-44                  line-card-module    48.00 C      normal
1/1-PHY-45-48                  line-card-module    49.00 C      normal
1/1-Switch-ASIC-Internal       line-card-module    56.25 C      normal

1/1-CPU-Zone-0                 management-module    50.00 C      normal
1/1-CPU-Zone-1                 management-module    50.00 C      normal
1/1-CPU-Zone-2                 management-module    50.00 C      normal
1/1-CPU-Zone-3                 management-module    51.00 C      normal
1/1-CPU-Zone-4                 management-module    51.00 C      normal
1/1-CPU-diode                  management-module    53.12 C      normal
1/1-DDR                        management-module    45.25 C      normal
1/1-Inlet-Air                  management-module    24.88 C      normal
1/1-MB-IBC                     management-module    45.62 C      normal
1/1-Switch-ASIC-diode          management-module    58.06 C      normal
```

Showing detailed temperature information for a 6300 switch:

```
switch# show environment temperature detail
Detailed temperature information
----------------------------------------------------------------
Mbr/Slot-Sensor       : 1/1-PHY-01-04
Module Type           : line-card-module
Module Description     : JL659A 6300M 48SR5 CL6 PoE 4SFP56 Swch
Status                : normal
Fan-state             : normal
Current temperature   : 45.00 C
Minimum temperature   : 41.00 C
Maximum temperature   : 50.00 C

Mbr/Slot-Sensor       : 1/1-PHY-05-08
Module Type           : line-card-module
Module Description     : JL659A 6300M 48SR5 CL6 PoE 4SFP56 Swch
Status                : normal
Fan-state             : normal
Current temperature   : 45.00 C
Minimum temperature   : 41.00 C
Maximum temperature   : 50.00 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
-e <EVENT-ID>	Shows the event logs for the specified event ID. Event ID range: 101 through 99999.
-s {emergency | alert | critical | error | warning | notice | info | debug}	Shows the event logs for the specified severity. Select the severity from the following list: ■ emergency: Displays event logs with severity emergency only. ■ alert: Displays event logs with severity alert and above. ■ critical: Displays event logs with severity critical and above. ■ error: Displays event logs with severity error and above. ■ warning: Displays event logs with severity warning and above. ■ notice: Displays event logs with severity notice and above. ■ info: Displays event logs with severity info and above. ■ debug: Displays event logs with all severities.
-r	Shows the most recent event logs first.
-a	Shows all event logs, including those events from previous boots.

Parameter	Description
`-n <COUNT>`	Displays the specified number of event logs.
`-i <MEMBER-SLOT>`	On a 6400: Shows the event logs for the specified slot ID.
`-i <MEMBER-SLOT>`	On a 6300: Shows the event logs for the specified VSF member ID.
`-m {active | standby}`	On a 6400: 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.
`-m {active | standby}`	On a 6300: Shows the event logs for the specified role. Selecting `active` displays the event log for the VSF conductor role and `standby` displays event logs for the VSF standby role.
`-c {lldp | ospf | ...}`	Shows the event logs for the specified event category. Enter `show event -c` for a full listing of supported categories with descriptions.
`-d {lldpd | bgpd | fand | ...}`	Shows the event logs for the specified process. Enter `show event -d` for a full listing of supported daemons with descriptions.

Examples

Showing event logs:

```
switch# show events
---------------------------------------------------
show event logs
---------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
    70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to
    up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1
    in Hardware
```

Showing the most recent event logs first:

```
switch# show events -r
---------------------------------------------------
show event logs
---------------------------------------------------
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1
    in Hardware
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to
    up for bridge_normal interface
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
    70:72:cf:51:50:7c
```

Showing all event logs:

```
switch# show events -a
---------------------------------------------------
```

```
show event logs
-------------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
    70:72:cf:51:50:7c
2016-12-01:12:37:31.734541|intfd|4001|INFO|AMM|1|Interface port_admin set to
    up for bridge_normal interface
2016-12-01:12:37:32.583256|switchd|24002|ERR|AMM|1|Failed to create VLAN 1
    in Hardware
```

Showing event logs related to LACP:

```
switch# show events -c lacp
--------------------------------------------------
show event logs
--------------------------------------------------
2016-12-01:12:37:31.733551|lacpd|15007|INFO|AMM|1|LACP system ID set to
    70:72:cf:51:50:7c
```

Showing event logs as per the specified management card role for a 6400 switch:

```
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

Not supported on the 6300 Switch Series.
```
show fabric [<SLOT-ID>] [vsx-peer]
```

Description

Shows information about the installed fabrics.

Parameter	Description
`<SLOT-ID>`	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`
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration 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 on Aruba 6400 switches that have two fabrics:

```
switch# show fabric

Fabric Modules
```

```
==============

      Product                                  Serial
Name  Number  Description                      Number     Status
----  ------- -------------------------------- ---------- ----------------
1/1   R0X25A  6410 Chassis                     SG9ZKM9999 Ready
1/2   R0X25A  6410 Chassis                     SG9ZKM9999 Ready
```

Showing all fabrics on Aruba 6400 switches that have one fabric:

```
switch# show fabric

Fabric Modules
==============

      Product                                    Serial
Name  Number  Description                        Number     Status
----  ------- ---------------------------------- ---------- ----------------
1/1   R0X24A  6405 Chassis                       SG9ZKM9076 Ready
```

Showing a single fabric module on Aruba 6400 switches:

```
switch# show fabric 1/1

Fabric module 1/1 is ready
Admin state: Up
Description: 6405 Chassis
Full Description: 6405 Chassis
Serial number: SG00000000
Product number: R0X24A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6400	Operator (>) or Manager (#)	Operators 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
myswitch
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show images

```
show images [vsx-peer]
```

Description

Shows information about the software in the primary and secondary images.

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

Example

Showing the primary and secondary images on a 6300 switch:

```
switch(config)# show images
-------------------------------------------------------------------------------
AOS-CX Primary Image
```

```
--------------------------------------------------------------------------------
Version : FL.xx.xx.xxxx
Size    : 722 MB
Date    : 2019-10-22 17:00:46 PDT
SHA-256 : 4c84e49c0961fc56b5c7eab064750a333f1050212b7ce2fab587d13469d24cfa


--------------------------------------------------------------------------------
AOS-CX Secondary Image
--------------------------------------------------------------------------------
Version : FL.xx.xx.xxxx
Size    : 722 MB
Date    : 2019-10-22 17:00:46 PDT
SHA-256 : 4c84e49c0961fc56b5c7eab064750a333f1050212b7ce2fab587d13469d24cfa

Default Image : secondary


--------------------------------------------------------------
Management Module 1/1 (Active)
--------------------------------------------------------------
Active Image       : secondary
Service OS Version : FL.01.05.0001-internal
BIOS Version       : FL.01.0001
```

Showing the primary and secondary images on a 6400 switch:

```
switch(config)# show images
--------------------------------------------------------------------------------
AOS-CX Primary Image
--------------------------------------------------------------------------------
Version : FL.xx.xx.xxxxQ-2710-gd4ac39f30c9
Size    : 766 MB
Date    : 2019-10-30 17:22:01 PDT
SHA-256 : e560ca9141f425d19024d122573c5ff730df2a9a726488212263b45ea00382cf


--------------------------------------------------------------------------------
AOS-CX Secondary Image
--------------------------------------------------------------------------------
Version : FL.xx.xx.xxxx
Size    : 722 MB
Date    : 2019-10-21 19:36:26 PDT
SHA-256 : 657e28adc1b512217ce780e3523c37c94db3d3420231deac1ab9aaa8324dc6b9

Default Image : secondary


--------------------------------------------------------------
Management Module 1/1 (Active)
--------------------------------------------------------------
Active Image       : secondary
Service OS Version : FL.01.05.0001-internal
BIOS Version       : FL.01.0001
```

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 [vsx-peer]
```

Description

Shows IP error statistics for packets received by the switch since the switch was last booted.

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

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 are 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 ip error statistics for packets received by the switch:

```
switch# show ip errors
--------------------------------
Drop reason              Packets
--------------------------------
Malformed packets              1
```

```
IP address errors              10
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400	Operator (>) or Manager (#)	Operators 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 (Aruba 6300 switch):

```
switch(config)# show module

Management Modules
==================

     Product                                       Serial
Name Number  Description                           Number     Status
---- ------- ------------------------------------- ---------- ----------------
1/1  JL659A  6300M 48SR5 CL6 PoE 4SFP56 Swch       ID9ZKHN090 Active (local)


Line Modules
============

     Product                                       Serial
Name Number  Description                           Number     Status
---- ------- ------------------------------------- ---------- ----------------
1/1  JL659A  6300M 48SR5 CL6 PoE 4SFP56 Swch       ID9ZKHN090 Ready
```

Showing a line module (Aruba 6400 switch):

```
switch# show module 1/3

Line module 1/3 is ready
 Admin state: Up
 Description: 6400 24p 10GT 4SFP56 Mod
 Full Description: 6400 24-port 10GBASE-T and 4-port SFP56 Module
 Serial number: SG9ZKMS045
 Product number: R0X42A
 Power priority: 128
```

Showing a slot that does not contain a line module:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show running-config

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

Description

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

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

Examples

Showing the current running configuration:

```
switch> show running-config
Current configuration:
!
!Version AOS-CX 10.0X.XXXX
!
lldp enable
linecard-module LC1 part-number JL363A
vrf green
!
!
!
```

```
!
!
!
aaa authentication login default local
aaa authorization commands default none
!
!
!
!
vlan 1
    no shutdown
vlan 20
    no shutdown
vlan 30
    no shutdown
interface 1/1/1
    no shutdown
    no routing
    vlan access 30
interface 1/1/32
    no shutdown
    no routing
    vlan access 20
interface bridge_normal-1
    no shutdown
interface bridge_normal-2
    no shutdown
interface vlan20
    no shutdown
    vrf attach green
    ip address 20.0.0.44/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable

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

    ip pim-sparse hello-interval 100
```

Showing the current running configuration in json format:

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

```
                         "medium_term_time_period": "120",
                         "short_term_high_threshold": "90",
                         "short_term_normal_threshold": "80",
                         "short_term_time_period": "5"
                     }
                 }
             },
...
...
...
...
```

Show the current running configuration without default values:

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

Show the current running configuration with default values:

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show running-config current-context

```
show running-config current-context
```

Description

Shows the current non-default configuration running on the switch in the current command context.

Usage

You can enter this command from the following configuration contexts:

- Any child of the global configuration (config) context. If the child context has instances—such as interfaces—you can enter the command in the context of a specific instance. Support for this command is provided for one level below the config context. For example, entering this command for a child of a child of the config context not supported. If you enter the command on a child of the config context,

the current configuration of that context and the children of that context are displayed.

- The global configuration (`config`) context. If you enter this command in the global configuration (`config`) context, it shows the running configuration of the entire switch. Use the `show running-configuration` command instead.

Examples

On the 6400 Switch Series, interface identification differs.

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
vlan access 1
    exit
```

Showing the current running configuration for the management interface:

```
switch(config-if-mgmt)# show running-config current-context
interface mgmt
    no shutdown
    ip static 10.0.0.1/24
    default-gateway 10.0.0.8
    nameserver 10.0.0.1
```

Showing the running configuration for the external storage share named `nasfiles`:

```
switch(config-external-storage-nasfiles)# show running-config current-context
external-storage nasfiles
    address 192.168.0.1
    vrf default
    username nasuser
    password ciphertext AQBapalKj+XMsZumHEwIc9OR6YcOw5Z6Bh9rV+9ZtKDKzvbaBAAAAB1CTrM=
    type scp
    directory /home/nas
    enable
switch(config-external-storage-nasfiles)#
```

Showing the running configuration for a context that does not have instances:

```
switch(config-vsx)# show run current-context
vsx
    inter-switch-link 1/1/1
    role secondary
    vsx-sync sflow time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show startup-config

```
show startup-config [json]
```

Description

Shows the contents of the startup configuration.

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

Parameter	Description
`json`	Display output in JSON format.

Examples

Showing the startup-configuration in non-JSON format for a 6300 switch:

```
switch(config)# show startup-config
Startup configuration:
!
!Version AOS-CX FL.xx.xx.xxxx
!export-password: default
hostname BLDG01-F1
user admin group administrators password ciphertext

AQBapWl8I2ZunZ43NE/8KlbQ7zYC4gTT6uSFYi6n6wyY9PdBYgAAACONCR/3+AcNvzRBch0DoG7W9z84LpJA
+6C9SKfNwCqi5/
nUPk/ZOvN91/EQXvPNkHtBtQWyYZqfkebbEH78VWRHfWZjApv4II9qmQfxpA79wEvzshdzZmuAKrm
user ateam group administrators password ciphertext

AQBapcPqMXoF+H10NKrqAedXLvlSRwf4wUEL22hXGD6ZBhicYgAAAGsbh70DKg1u+Ze1wxgmDXjkGO3bseYi
R3LKQg66vrfrqR/
M3oLlliPdZDnq9XMMvCL+7jBbYhYes8+uDxuSTh8kdkd/qj3lo5FUuC5fENgCjU0YI1l7qtU+YEnsj
!
!
!
!
radius-server host 10.10.10.15
!
radius dyn-authorization enable
ssh server vrf default
ssh server vrf mgmt
!
!
!
!
!
router ospf 1
```

```
    router-id 1.63.63.1
    area 0.0.0.0
vlan 1
vlan 66
    name vlan66
vlan 67
    name vlan67
vlan 999
    name vlan999
vlan 4000
spanning-tree
interface mgmt
    no shutdown
    ip static 10.6.9.15/24
    default-gateway 10.6.9.1
```

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
`basic <PORT-NUM>`	Specifies a physical port on the switch. Use the format `member/slot/port` (for example, `1/3/1`).
`extended`	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
6300 6400	Manager (#)	Administrators or local user group members with execution rights for this command.

show system

```
show system [vsx-peer]
```

Description

Shows general status information about 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

CPU utilization represents the average utilization across all the CPU cores.

System Contact, System Location, and System Description can be set with the `snmp-server` command.

Examples

Showing system information on a 6300 switch:

```
switch(config)# show system
Hostname           : switch
System Description : FL.10.xx.xxxxx
System Contact     :
System Location    :

Vendor             : Aruba
Product Name       : JL659A 6300M 48SR5 CL6 PoE 4SFP56 Swch
Chassis Serial Nbr : ID9ZKHN090
Base MAC Address   : 9020c2-245080
AOS-CX Version : FL.10.xx.xxxx

Time Zone          : UTC

Up Time            : 5 days, 15 hours, 33 minutes
CPU Util (%)       : 21
Memory Usage (%)   : 19
```

Showing system information om a 6400 switch:

```
switch(config)# show system
Hostname          : switch
System Description : FL.10.xx.xxxxx
System Contact    :
System Location   :

Vendor            : Aruba
Product Name      : R0X24A 6405 Chassis
Chassis Serial Nbr : SG9ZKM7206
Base MAC Address  : 9020c2-dc4700
AOS-CX Version : FL.10.xx.xxxxx

Time Zone         : UTC

Up Time           : 32 minutes
CPU Util (%)      : 3
Memory Usage (%)  : 10
BLDG02-F3(config)#
```

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 system resource-utilization

```
show system resource-utilization [daemon <DAEMON-NAME> | all | module <SLOT-ID> | standby]
[vsx-peer]
```

Description

Shows information about the usage of system resources such as CPU, memory, and open file descriptors.

Parameter	Description
daemon <DAEMON-NAME>	Shows the filtered resource utilization data for the process specified by <DAEMON-NAME> only.
vrf <VRF-NAME>	Specifies the VRF name to be used for communicating with the server. If no VRF name is provided, the default VRF named default is used. **NOTE:** For a list of daemons that log events, enter show events -d ? from a switch prompt in the manager (#) context.

Parameter	Description
`all`	Shows utilization information for all VSF members.
`module <SLOT-ID>`	Shows the filtered resource utilization data for the line module specified by `<SLOT-ID>` only.
`vsx-peer`	Shows the output from the VSX peer switch. If the switches do not have the VSX configuration 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 system resource utilization data:

```
switch# show system resource-utilization
System Resources:
Processes: 70
CPU usage(%): 20
Memory usage(%): 25
Open FD's: 1024

Process             CPU Usage(%)          Memory Usage(%)    Open FD's
-----------------------------------------------------------------------
pmd                 2                     1                  14
hpe-sysmond         1                     2                  11
hpe-mgmdd           0                     1                  5
...
```

Showing the resource utilization data for the pmd process:

```
switch# show system resource-utilization daemon pmd
Process             CPU Usage             Memory Usage      Open FD's
-----------------------------------------------------------------------
pmd                 2                     1                  14
```

Showing resource utilization data when system resource utilization polling is disabled:

```
switch# show system resource-utilization
System resource utilization data poll is currently disabled
```

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(%): 0
Memory usage(%): 35
Open FD's: 512
```

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 tech

```
show tech [basic | <FEATURE>] [local-file]
```

Description

Shows detailed information about switch features by automatically running the `show` commands associated with the feature. If no parameters are specified, the `show tech` command shows information about all switch features. Technical support personnel use the output from this command for troubleshooting.

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

Usage

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

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

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

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

Example

Showing the basic set of system information:

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


******************************
Command : show core-dump all
******************************
no core dumps are present
```

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


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

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show usb

```
show usb [vsx-peer]
```

Description

Shows the USB port configuration and mount settings.

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

Examples

If USB has not been enabled:

```
switch> show usb
Enabled: No
Mounted: No
```

If USB has been enabled, but no device has been mounted:

```
switch> show usb
Enabled: Yes
Mounted: No
```

If USB has been enabled and a device mounted:

```
switch> show usb
Enabled: Yes
Mounted: Yes
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with 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 a 6300 switch:

```
6300# show version
-------------------------------------------------------------------------------
ArubaOS-CX
(c) Copyright 2017-2022 Hewlett Packard Enterprise Development LP
-------------------------------------------------------------------------------
Version       : FL.10.10.0001BJ
Build Date    : 2022-05-25 10:22:06 UTC
Build ID      : ArubaOS-CX:FL.10.10.0001BJ:16d4d3ca52e9:202205908
Build SHA     : 16d4d349695b50298f34b21a8c67637ae0
Hot Patches   : hpe-routing_FL_10_10_0001BJ.patch
Active Image  : primary

Service OS Version : FL.01.11.0001-internal
BIOS Version       : FL.01.0004
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

system resource-utilization poll-interval

```
system resource-utilization poll-interval <SECONDS>
```

Description

Configures the polling interval for system resource information collection and recording such as CPU and memory usage.

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

Example

Configuring the system resource utilization poll interval:

```
switch(config)# system resource-utilization poll-interval 20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

top cpu

```
top cpu
```

Description

Shows CPU utilization information.

Example

Showing top CPU information:

```
switch# top cpu
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks:  76 total, 2 running, 74 sleeping,  0 stopped,  0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total,  2487508 free,  897040 used,   661948 buff/cache
KiB Swap:       0 total,       0 free,       0 used,  2859196 avail Mem

  PID USER     PRI  NI   VIRT    RES   SHR S  %CPU %MEM     TIME+ COMMAND
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

top memory

```
top memory
```

Description

Shows memory utilization information.

Example

Showing top memory:

```
switch> top memory
top - 09:42:55 up 3 min, 3 users, load average: 3.44, 3.78, 1.70
Tasks:  76 total, 2 running, 74 sleeping,  0 stopped,  0 zombie
%Cpu(s): 31.4 us, 32.7 sy, 0.5 ni, 34.4 id, 04. wa, 0.0 hi, 0.6 si, 0.0 st
KiB Mem : 4046496 total,  2487508 free,  897040 used,   661948 buff/cache
KiB Swap:       0 total,        0 free,        0 used,  2859196 avail Mem

  PID USER     PRI  NI   VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
...
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

usb

```
usb
no usb
```

Description

Enables the USB ports on the switch. This setting is persistent across switch reboots and management module failovers. Both active and standby management modules are affected by this setting.

The no form of this command disables the USB ports.

Example

Enabling USB ports:

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

Disabling USB ports when a USB drive is mounted:

```
switch(config)# no usb
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

usb mount | unmount

```
usb {mount | unmount}
```

Description

Enables or disables the inserted USB drive.

Parameter	Description
`mount`	Enables the inserted USB drive.
`unmount`	Disables the inserted USB drive in preparation for removal.

Usage

If USB has been enabled in the configuration, the USB port on the active management module is available for mounting a USB drive. The USB port on the standby management module is not available.

An inserted USB drive must be mounted each time the switch boots or fails over to a different management module.

A USB drive must be unmounted before removal.

The supported USB file systems are FAT16 and FAT32.

Examples

Mounting a USB drive in the USB port:

```
switch# usb mount
```

Unmounting a USB drive:

```
switch# usb unmount
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm
Aruba Support Portal	https://asp.arubanetworks.com/
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
AOS-CX Switch Software Documentation Portal	https://www.arubanetworks.com/techdocs/AOS-CX/help_portal/Content/home.htm

Aruba Hardware Documentation and Translations Portal	https://www.arubanetworks.com/techdocs/hardware/DocumentationPortal/Content/home.htm
Aruba software	https://asp.arubanetworks.com/downloads
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba Developer Hub	https://developer.arubanetworks.com/

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

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://asp.arubanetworks.com/notifications/subscriptions (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP 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

Aruba 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

Aruba 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.