

AOS-CX 10.09 Monitoring Guide

6200 Switch Series



Copyright Information

© Copyright 2023 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Notices

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

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

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

Acknowledgment

Intel®, Itanium®, Optane™, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

All third-party marks are property of their respective owners.

Contents	3
About this document	6
Applicable products	6
Latest version available online	6
Command syntax notation conventions	6
About the examples	7
Identifying switch ports and interfaces	7
Monitoring hardware through visual observation	9
Confirming normal operation of the switch by reading LEDs	9
Detecting if the switch is not ready for a failover event	10
Finding faulted components using the switch LEDs	10
Switch and port LEDs for 6200 Switch Series	12
Boot commands	15
boot set-default	15
boot system	15
show boot-history	17
Switch system and hardware commands	20
External storage	21
External storage commands	21
address (external storage)	21
directory	22
disable external-storage logfiles	23
enable (external-storage logfiles)	23
external-storage	24
password (external-storage)	25
show external-storage	26
show running-config external-storage	27
type (external storage)	27
username (external storage)	28
vrf (external storage)	29
IP-SLA	31
IP-SLA guidelines	31
Limitations with VoIP SLAs	32
IP-SLA commands	32
ip-sla responder	32
show ip-sla responder	33
show ip-sla responder results	34
L1-100Mbps downshift	35
Limitations with speed downshift	35

L1-100Mbps downshift commands	35
downshift enable	35
show interface	36
show interface downshift-enable	39
show running-config interface	39
Mirroring	42
Mirror statistics	42
Classifier policies and mirroring sessions	42
VLAN as a source	43
Mirroring commands	43
clear mirror	43
comment	44
copy tcpdump-pcap	45
copy tshark-pcap	46
destination cpu	47
destination interface	48
destination tunnel	48
diagnostic	50
diag utilities tcpdump	51
disable (mirror session)	53
enable (mirror session)	54
mirror session	55
show mirror	55
source interface	57
source vlan	59
Monitoring a device using SNMP	61
Power-over-Ethernet	62
PoE commands	63
lldp dot3 poe	63
lldp med poe	64
power-over-ethernet	64
power-over-ethernet allocate-by	65
power-over-ethernet always-on	66
power-over-ethernet assigned-class	67
power-over-ethernet pre-std-detect	68
power-over-ethernet priority	68
power-over-ethernet quick-poe	69
power-over-ethernet threshold	70
power-over-ethernet trap	71
show lldp local	72
show lldp neighbor	72
show power-over-ethernet	73
Aruba AirWave	78
SNMP support and AirWave	78
SNMP on the switch	78
Supported features with AirWave and the AOS-CX switch	79
Configuring the AOS-CX switch to be monitored by AirWave	79
Support and Other Resources	81
Accessing Aruba Support	81
Accessing Updates	82
Aruba Support Portal	82

My Networking	82
Warranty Information	82
Regulatory Information	82
Documentation Feedback	83

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 6200 Switch Series (JL724A, JL725A, JL726A, JL727A, JL728A)

Latest version available online

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

Command syntax notation conventions

Convention	Usage
<code>example-text</code>	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets ([]).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: <ul style="list-style-type: none">▪ <code><example-text></code>▪ <code><example-text></code>▪ <i>example-text</i>▪ <i>example-text</i>	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: <ul style="list-style-type: none">▪ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value.▪ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.
	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[]	Brackets. Indicates that the enclosed item or items are optional.

Convention	Usage
... or . . .	Ellipsis: <ul style="list-style-type: none"> ■ 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 6200 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 8. 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 in slot 1 on member 1.

Confirming normal operation of the switch by reading LEDs

This task describes using the switch LEDs to confirm that the switch is operating normally.

Procedure

1. Quick check: Verify that the chassis has power and there are no fault conditions.
On the front of the switch, verify that the states of the following LEDs are On Green:
 - Power
 - Health
2. Verify that the Health LEDs of all installed line modules are On Green.
3. Verify that the Health LEDs of all installed management modules are On Green.
4. Verify that the network ports are operating normally.
 - a. On the active management module, check the Status Front section. Verify that each LED that indicates a line module is in one of the following states:
 - On Green (normal operation)
 - Off (no line module installed)
 - b. On each line module, verify that each port LED is in one of the following states:
 - On Green, Half-Bright Green, or Flickering Green (normal operation)
 - Off (no cable connected or port off by default in config)
5. Verify that the power supplies are operating normally.
 - a. On the active management module, check the Status Front section. Verify that each LED that indicates a power supply is in one of the following states:
 - On Green (normal operation)
 - Off (no power supply installed)
 - b. On each power supply, verify that LEDs are in the following states:
 - Power LED: On Green
 - Fault LED: Off
6. Verify that the rear components are operating normally by checking the Status Rear section of the active management module:
 - a. Verify that the LEDs for the fabric modules are in one of the following states:
 - On Green (normal operation)
 - Off (component not installed)
 - b. Verify that the LEDs for the fan trays and fans are On Green.
7. Verify that the standby management module is ready to take over as the active management module. On the standby management module, verify the states of the following LEDs:

- Health LED is On Green.
- Management state standby (Stby) LED is On Green.

Detecting if the switch is not ready for a failover event

This task describes using the switch LEDs to detect if the switch is not ready for the loss of a fabric module or for a failover from the active management module to the standby management module.



Although you can detect power supply failures by viewing the LEDs, you must use software commands to determine if the power supply redundancy is sufficient to power the chassis if a power supply fails.

Procedure

1. Detect if the standby management module is shut down.
If the standby management module is shut down, the LED states are as follows:
 - The standby management module health LED is Off.
 - The standby management state active (Actv) LED is Off.
 - The standby management state standby (Stby) LED is Off.
 - On the active management module in the Status Front Management Modules section, the LED for the standby management module is Off. For example, if the active management module is Management Module LED 5, Management Modules LED 6 is Off.
2. Detect if the standby management module is in a transient state. If the standby management module is booting, updating, or in another transient state, the LED states are as follows:
 - The standby management module health LED is Slow Flash Green when the service operating system is running or during an operating system update.
 - The standby management module Booting LED is Slow Flash Green when the AOS-CX operating system is booting.
 - The standby management state active (Actv) LED is Off.
 - The standby management state standby (Stby) LED is Off.
 - On the active management module in the Status Front Management Modules section, the LED for the standby management module is Slow Flash Green.
3. Detect if a fabric module is shut down or not present. If a fabric module is shut down or not present, the LED states are as follows:
 - On the active management module, in the Status Rear section, the LED for the fabric module is Off.
 - On the rear display module, the LED for the fabric module is Off.
 - On the fabric module, the health LED is Off. However, the fabric module is behind fan 1 and is not directly visible.

Finding faulted components using the switch LEDs

This task describes using the switch LEDs to find components that are in a fault condition.



All green LEDs—except for chassis power LEDs and the Usr1 LED—are off when the LED mode is set to Light Faults (The Usr1 LED of the LED Mode section of the active management module is On Green and the default behavior for the Usr1 LED is being used.).

Procedure

1. Find the switch that has the fault condition, which is indicated by a chassis health LED in the state of Slow Flash Orange.

The chassis health LED is located on the front of the switch and on the rear panel of the switch.

2. If you are at the back of the switch, on the rear panel, look for LEDs that are in the Slow Flash Orange state:

The Status Rear area has LEDs for power supplies, fabric modules, fan trays, and fans. The number on the LED represents the unit number of the component.

If the only LED in a state of Slow Flash Orange is the Chassis health LED, go to the front of the switch.

3. At the front of the switch, on the active management module, look for LEDs that are in the Slow Flash Orange state:
 - The Status Front area has LEDs for power supplies, line and fabric modules, and management modules. The number on the LED indicates the slot number of the component.
 - The Status Rear area has LEDs for fabric modules and fan trays, with a single LED for all the fans in the fan tray. The number on the LED represents the slot or bay number of the component.

4. Use the number indicated by the LED that is flashing to locate the slot that contains the faulted component.

The fabric modules are located behind the fan trays, and the fabric module number corresponds to the fan tray number.

5. At the front of the switch, on line modules, look for LEDs that are in the Slow Flash Orange state: Module LEDs and Port LEDs indicate faults if their states are Slow Flash Orange.

Figure 1 *Switch and Port LEDs*

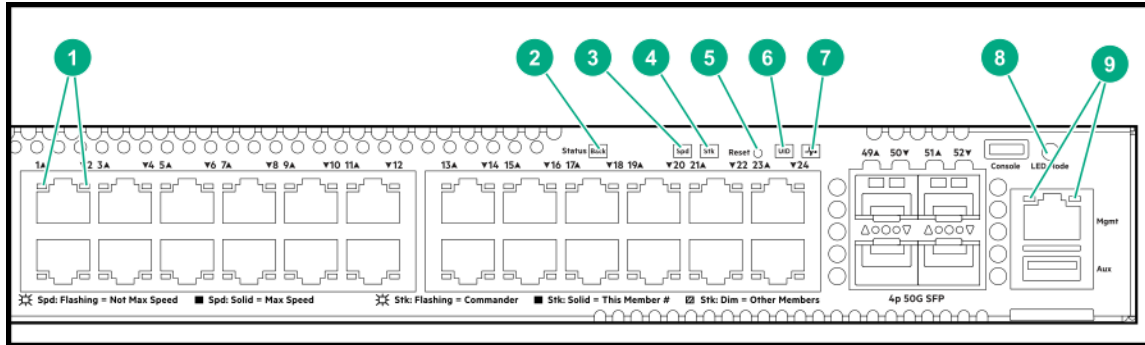


Table 1: *Switch and port LEDs: Labels and description*

Label	Description
1	Switch port LEDs
2	Back Module status LED
3	Speed mode selected LED
4	PoE mode selected
5	Reset button Usr mode selected LED
6	UID (Unit Identification)
7	Global Status LED
8	LED Mode status LED
9	Management Console LED

Table 2: *Front panel LED behavior*

Switch LEDs	Function	State	Meaning
Back LED	Status of modular components installed in the back of the chassis (not applicable for 6200F/6300F switches)	On - Green	Normal
		Slow Flash - Amber	Fault in one of the modules in the back of the chassis

Switch LEDs	Function	State	Meaning
PoE LED	Indicates Port LEDs are showing PoE information (not applicable for non PoE switches)	Off	PoE mode not selected
		On - Green	PoE mode selected
		Slow Flash - Amber	Hardware failure PoE enabled port, PoE mode not selected
		On - Amber	Hardware failure PoE enabled port, PoE mode selected
Spd LED	Indicates Port LEDs are showing speed information	Off	Speed mode not selected
		On - Green	Speed mode selected
		Not Implemented	No fault defined
Stk LED	Indicates Port LEDs are showing stacking mode information	Off	Stacking mode not selected
		On - Green	Stacking mode selected
		On - Amber	A port has a stacking failure. Stacking mode selected
		Slow flash Amber	A port has a stacking failure. Stacking mode not selected
UID LED	User-configurable LED	Off	User defined the located LED : OFF
		On/Flash Blue (for 30 min)	User defined the locator LED: On/Flash
Global Status Indicator LED	Overall status of the product	Flash - Green	Self-test in progress during UBOOT, SVOS and AOS-CX
		On - Green	Successfully initialized AOS-CX
		Flash - Amber	Recoverable faults (e.g. fans, PSU fault)
		On - Amber	Critical faults (e.g. exceed temperature limit)
OOBM Status Indicator LED	Status of OOBM Link connectivity	Off	OOBM port is not connected, no link established
		Half Bright - Green	OOBM port is enabled and established link with partner

Switch LEDs	Function	State	Meaning
		On - Green	Experiencing high bandwidth utilization
		Activity Flicker - Green	% of the time that the LED light up is roughly proportional to the % of full bandwidth utilization of the port
* Press the Mode Select button to switch between User(default), PoE, Spd, or Stk Mode.			

Table 3: Rear panel LED behavior

Switch LEDs	Function	State/Mode	Meaning
Fan health LED	Status of fan	On - Green	Normal
		Slow flash - Amber	Fan fault
UID LED	User-configurable LED	Off	User define the locator LED : OFF
		On/Flash (30 min) - blue	User define the locator LED: On/Flash
PSU Status Indicator LED	Status of power supply	On Green	Normal
		Off	No power, PSU has invalid AC input of invalid DC outputs
		Slow Flash - Green	Power supply has faulted or warning

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

Usage

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

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

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

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

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

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

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

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

Examples

Rebooting the system from the configured default operating system image:

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

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

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
<code>all</code>	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.

Switch system and hardware commands are general commands used to configure fundamental settings on the switch.



Refer to the Fundamentals Guide to view the switch system and hardware commands.

The switch has limited capacity to store data, collected by switch features and protocols. You can provide virtually unlimited storage capacity by adding user-supplied external storage volumes. Supported volume types and storage protocols include: NFSv3, NFSv4, and SCP (sshfs).

One application of external storage is the saving and restoring of DHCP lease files over SCP or NFS network attached storage systems. SCP file system protocol uses a user mode process to emulate a network file system. The key advantage is packet level encryption and simple configuration. The key disadvantage is slow performance.

You can set up external storage volume credentials and then enable it. A storage management process acts on your requests by enabling the storage volume using the requested storage protocol. You can disable the external storage volume or set it up but leave it disable.

The feature maintains storage volume state. The states are: **disabled** (down), **connecting** (establishing connection), **operational** (up), and **unaccessible** (unavailable).

If a storage volume is unavailable, the system attempts to reconnect periodically. Multiple volumes could connect concurrently. If one connection times out the others can connect immediately.

The system supports server connection through data and management ports.

Data port support requires server IP address on a default VRF.

Once a storage volume is enabled, applications can use the volume to store retrieve and delete files and directories.

External storage commands

address (external storage)

```
address {<IPV4-ADDR> | <IPV6-ADDR> | hostname <HOSTNAME>}  
no address {<IPV4-ADDR> | <IPV6-ADDR> | hostname <HOSTNAME>}
```

Description

Specifies the NAS IP address or hostname.

The `no` form of this command deletes an IP address or hostname.

Parameter	Description
<IPV4-ADDR>	Specifies the NAS server IPv4 address, Global.
<IPV6-ADDR>	Specifies the IPv6 address of the NAS server.
<HOSTNAME>	Specifies the hostname of the NAS server. String.

Examples

Creating the logfiles storage volume with IP address 10.1.1.1:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# address 10.1.1.1
```

Deleting an external storage volume named logfiles:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# no address 10.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage-<VOLUME-NAME>	Administrators or local user group members with execution rights for this command.

directory

```
directory <DIRECTORY-NAME>  
no directory <DIRECTORY-NAME>
```

Description

Selects an existing directory on the external storage volume.

The `no` form of this command clears a directory of an external storage volume.

Parameter	Description
<DIRECTORY-NAME>	Specifies the external storage directory for mapping the volume.

Examples

Creating a volume named logfiles that is mapped under /home on the server:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# directory /home
```

Clearing the directory /home:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# no directory /home
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage-<VOLUME-NAME>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

disable external-storage logfiles

disable
no disable

Description

Disables the external storage volume.

The `no` form of this command enables the external storage volume. This is identical to the `enable` command.

Examples

Disabling a volume named logfiles:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage-<VOLUME-NAME>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

enable (external-storage logfiles)

enable
no enable

Description

Enables the external storage volume.

The `no` form of this command disables the external storage volume. This is identical to the `disable` command.

Examples

Creating and then enabling a volume named logfiles:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# enable
```

Disables the external storage volume:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage- <i><VOLUME-NAME></i>	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

external-storage

```
external-storage <VOLUME-NAME>
no external-storage <VOLUME-NAME>
```

Description

Creates or updates an external storage volume.

The `no` form of this command deletes an external storage volume.

Examples

Creating the logfiles storage volume:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)#
```

Deleting the logfiles storage volume:

```
switch(config)# no external-storage logfiles
```


Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Administrators or local user group members with execution rights for this command.

password (external-storage)

```
password [{plaintext | ciphertext} <PASSWORD>]  
no password {plaintext | ciphertext} <PASSWORD>
```

Description

Sets the password for network attached storage server login.

The `no` form of this command clears the password for network attached storage server login.

Parameter	Description
{ciphertext plaintext}	Selects the password format.
<PASSWORD>	Specifies the password. NOTE: When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Creating a volume named logfiles with password Xj#9:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# password plaintext Xj#9
```

Creating a volume named bak1 with a prompted plaintext password:

```
switch(config)# external-storage bak1  
switch(config-external-storage-bak1)# password  
Enter the NAS server password: *****  
Re-Enter the NAS server password: *****
```

Clearing the password for volume logfiles:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# no password plaintext Xj#9
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage-<VOLUME-NAME>	Administrators or local user group members with execution rights for this command.

show external-storage

show external-storage [<VOLUME-NAME>]

Description

Shows external storage configuration and state for all volumes or for a specified volume.

Parameter	Description
<VOLUME-NAME>	Specifies the external storage volume name that the show command will use.

Examples

```
switch# show external-storage
-----
--
      Address      VRF      Username      Type      Directory      State
-----
--
nfsvol   10.1.1.1      nas      ---           NFSv3      /home
operational
nfsfiles 20.1.1.1      nas      netstorage    NFSv4      /netstor      disabled
scpdev   nasserver     nas      scpstor       SCP        /scp
unaccessible
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show running-config external-storage

show running-config external-storage

Description

Shows the running configuration of the external storage.

Examples

```
switch# show running-config external-storage

external-storage nfsvol
  address 10.1.1.1
  vrf     nas
  type    nfsv4
  directoty /home
  enable
external-storage scpdev
  address 30.1.1.1
  vrf     nas
  username switchuser
  password ciphertext xxx
  type    scp
  directoty /home
  enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

type (external storage)

```
type {nfsv3 | nfsv4 | scp}
no type {nfsv3 | nfsv4 | scp}
```

Description

Sets the network attached storage access type for reaching the external storage volume.

The `no` form of this command deletes an external storage volume.

Parameter	Description
nfsv3	Specifies the NFSv3 network access protocol.
nfsv4	Specifies the NFSv4 network access protocol.
scp	Specifies the SCP network access protocol.

Examples

Creating the logfiles volume using NFSV4:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# type nfsv4
```

Clearing the external storage access type:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no type nfsv4
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage- <i><VOLUME-NAME></i>	Administrators or local user group members with execution rights for this command.

username (external storage)

```
username <USER-NAME>
no username <USER-NAME>
```

Description

Sets the username for logging in to a network attached storage server.

The `no` form of this command clears a username.

Parameter	Description
<i><USER-NAME></i>	Specifies the username.

Examples

Creating a volume named logfiles with the user name nassuser:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# username nassuser
```

Clearing the user name nassuser from accessing the logfiles volume:

```
switch(config)# external-storage logfiles
switch(config-external-storage-logfiles)# no username nassuser
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage-<VOLUME-NAME>	Administrators or local user group members with execution rights for this command.

vrf (external storage)

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

Description

Setting a VRF to reach network attached storage.

The `no` form of this command clears access of a VRF to network attached storage.

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

Examples

Creating the logfiles volume and setting a VRF named `nas` to access the network attached storage:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# vrf nas
```

Clearing access of a VRF named `nas` to the network attached storage:

```
switch(config)# external-storage logfiles  
switch(config-external-storage-logfiles)# no vrf nas
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-external-storage-<VOLUME-NAME>	Administrators or local user group

Platforms	Command context	Authority
		members with execution rights for this command.

The IP Service Level Agreement (IP-SLA) is a feature that enables the measuring of network performance between two nodes in a network for different service level agreement parameters such as round-trip time (RTT), one-way delay, jitter, reachability, packet loss, and voice quality scores. These two nodes can span across area in access, distribution or core inside a LAN as well as across WAN between core to core or core to Data Centre switches. This feature helps you measure the SLA for different protocols or applications such as UDP echo, UDP jitter (for voice and video), TCP connect, HTTP, and ICMP echo. This guide provides details for managing and monitoring different types of IP-SLAs.

IP-SLA guidelines

- AOS-CX supports only SLA configuration through CLI and thresholds can be configured using NAE agents using WebUI/REST.
- AOS-CX supports only forever tests. On-demand tests are not supported.
- Maximum sessions: IP-SLA source 50, IP-SLA responder 80.
- NAE can effectively monitor a maximum of 300 parameters, reducing the maximum supported session by 300.
- NAE supports only syslog.
- NAE agents must be triggered for each IP-SLA test on every switch.
- If multiple IP addresses are received for a DNS query, DNS works with the first resolved IP.
- When the DNS server IP is not configured, the first DNS server in `resolve.conf` is used.
- The source interface/IP option is not applicable for SLAs configured on 'mgmt' VRF, as it has only one interface.
- A system time change because of NTP or a manual change causes an incorrect calculation.
- There is no interoperability of UDP echo SLA between AOS-CX and FlexFabric switches.
- Source IP and source port combination must be unique across SLA sessions in a same switch.
- Do not use the same source port across the source and responder sessions in a switch.
- NTP synchronization is a must for SLA types involving one-way delay such as UDP jitter VoIP.
- It is mandatory to set default CoPP to the max value when UDP jitter SLA is enabled otherwise 100% packet loss can be seen and `UDP-Jitter sla probe` will result in failure as seen in the following example.

```
copp-policy default
  class hypertext priority 6 rate 50000 burst 64
  default-class priority 6 rate 99999 burst 9999
```

- Deviations with respect to PVOS results: The packet losses due to internal switch-related issues like interface shutdown or interface flaps will not be considered as 'Probes Timed-out error', as the IP-SLA solution is to measure network performance and anomalies. Rather, this kind of packet loss will be counted in internal counters like 'Destination address unreachable'.

Limitations with VoIP SLAs

- A maximum of 80 concurrent VoIP SLAs can be scheduled in a 20 second slot.
- A single VoIP probe takes 20 seconds to complete.
- The default and minimum probe interval for VoIP SLA is 120 seconds.
- SLAs scheduled in the same slot, periodically sends 1000 probe packets for 120 seconds in 20 second intervals.
- Default 120 second probe interval is divided in to 6 slots of 20 seconds to avoid synchronization of all configured VoIP SLAs sending probes at the same time.
- SLAs started at the same time exceeding the concurrent limit of 80 must wait for the next 20 second VoIP slot to open before moving to 'running' state.
- The maximum number of VoIP SLAs supported is 80 X 6 slots = 480 SLAs.
- SLAs exceeding 480 will continue to remain in the 'waiting for VoIP slot' until any slot is freed by stopping the running SLA.
- To avoid high RTT, a single switch with more than 20 SLAs should not have single responder SLA.
- When IP is received dynamically (e.g. using DHCP) for interfaces other than management interface, IPSLA source or responder has to be configured only using interface name.

IP-SLA commands

ip-sla responder

```
ip-sla responder <SLA-NAME> {udp-echo | tcp-connect | udp-jitter-voip} <PORT-NUM>
    [source {<SOURCE-IPV4-ADDR> | <IFNAME>}][vrf <VRF-NAME>]
no ip-sla responder <SLA-NAME> {udp-echo | tcp-connect | udp-jitter-voip} <PORT-NUM>
    [source {<SOURCE-IPV4-ADDR> | <IFNAME>}][vrf <VRF-NAME>]
```

Description

Selects the IP-SLA responder. The responder can be configured for udp-echo, tcp-connect, udp-jitter-voip type. It requires the SLA name, SLA type, and port number as arguments. Source IP/interface ID is a must for type udp-jitter-voip and optional for other types.

The `no` form of this command removes the IP-SLA responder.

Parameter	Description
<SLA-NAME>	Specifies the SLA name.
udp-echo	Enables responder for udp-echo probes.
tcp-connect	Selects TCP connect as the IP-SLA test mechanism.
vrf <VRF-NAME>	Specifies the name of the VRF to use.
udp-jitter-voip	Selects VOIP jitter as the IP-SLA test mechanism.
<PORT-NUM>	Specifies the port number to listen for IP-SLA probes. Range: 1 to 65535.
[source {<SOURCE-IPV4-ADDR> <IFNAME>}]	Selects the source IPv4 address for SLA probes or the source interface to use for sending IP-SLA probes.

Examples


```
switch(config)# ip-sla responder SLA1 udp-echo 8000 source 2.2.2.2
switch(config)# ip-sla responder SLA1 udp-echo 8000 source 1/1/1
```

```
switch(config)# no ip-sla responder SLA1 udp-echo 8000 source 2.2.2.2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Administrators or local user group members with execution rights for this command.

show ip-sla responder

```
show ip-sla responder <SLA-NAME>
```

Description

Shows the given IP-SLA responder configuration and operation status.

Parameter	Description
<SLA-NAME>	Specifies the SLA name.

Examples

```
switch(config)# show ip-sla responder SLA3

SLA Name           : SLA3
IP-SLA Type        : Udp-echo
VRF                 : Default
Responder Port      : 8000
Responder IP        : 2.2.2.3
Responder Interface : 1/1/1
Responder Status    : Running
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Administrators or local user group members with execution rights for this command.

show ip-sla responder results

```
show ip-sla responder <SLA-NAME> <SOURCE-IPV4-ADDR> <PORT-NUM> results
```

Description

Shows the given ip-sla responder statistics for a given source IP and port. This command is only applicable for the sources where source IP and port are configured.

Parameter	Description
<SLA-NAME>	Specifies the SLA name.
<SOURCE-IPV4-ADDR>	Specifies the source IPV4 address.
<PORT-NUM>	Specifies the port number. Range: 1 to 65535.

Examples

```
switch# show ip-sla responder SLA1 2.2.2.1 8000 results

IP-SLA Type       : Udp-echo
VRF Name          : Default
Source IP         : 2.2.2.1
Source Port       : 8000
Responder Port    : 8888
Responder IP      : 2.2.2.3
Responder Interface :
Responder Status  : Running
Packets Received  : 2
Packets Sent      : 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Administrators or local user group members with execution rights for this command.

The speed downshift feature allows the user to link-up at sub-optimal speeds when failing to link-up at the highest advertised speed. There are fixed number of link attempts made to establish link at highest advertised speed and when all of them fail and attempt is made to link-up at a lower possible speed.

This feature requires underlying PHY to have support for the same and hence capability is only added to select set of ports. If a link cannot be established at the highest common denominator within a set number of link attempts, the PHY advertises the next highest speed using auto-negotiation.

Limitations with speed downshift

- Link up may be delayed as certain number of retries are done to establish the link at highest advertise speeds by both link partners before downshifting.
- Link may be established at sub-optimal speed.

L1-100Mbps downshift commands

downshift enable

```
downshift-enable  
no downshift-enable
```

Description

Enables/disables automatic speed downshift on an interface that supports downshift, generally 1GBASE-T ports. When enabled, downshift allows an interface to link at a lower advertised speed when unable to establish a stable link at the maximum speed. Downshifting only applies to physical interfaces that are not members of a LAG and is only available when auto-negotiation is enabled. When only one speed is advertised, downshift will not be triggered.

Examples

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

```
Warning: this is a non-standard mode for use only when standards-based  
auto-negotiation is not able to establish a stable link. Enabling this  
may cause the port to link at a lower than expected speed and should  
not be used on ports that are members of a LAG. Support calls may require  
this feature to be disabled
```

```
Continue (y/n)?
```

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

When automatic downshift is enabled:

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

Disabling automatic speed downshift:

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

show interface

```
show interface [<IFNAME>|<IFRANGE>] [brief | physical | extended [non-zero]]
show interface [lag | loopback | tunnel | vlan ] [<ID>] [brief | physical]
show interface [lag | loopback | tunnel | vlan ] [<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.
non-zero	Shows only non zero statistics.
LAG	Shows LAG interface information.
LOOPBACK	Shows loopback interface information.
TUNNEL	Shows tunnel interface information.

Parameter	Description
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

The following example shows when interface 1/1/1 is configured:

```
switch# show interface 1/1/1
Interface 1/1/1 is up
Admin state is up
Link state: up for 1 minute (since Thu Nov 26 10:26:34 UTC 2020)
Link transitions: 3
Description:
Hardware: Ethernet, MAC Address: 88:3a:30:47:d1:df
MTU 1500
Type 1GbT
Full-duplex
qos trust cos
Speed 1000 Mb/s
Auto-negotiation is on
Energy-Efficient Ethernet is disabled
Flow-control: off
Error-control: off
MDI mode: MDIX
VLAN Mode: native-untagged
Native VLAN: 1
Allowed VLAN List: all
Rate collection interval: 300 seconds

Rates
-----
Mbits / sec           RX           TX           Total (RX+TX)
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
-----
Packets               RX           TX           Total
  Unicast              0           0           0
  Multicast            0           0           0
  Broadcast            0           0           0
Bytes                 0           0           0
Jumbos                0           0           0
Dropped               0           0           0
Filtered              0           0           0
```

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

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
```

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
```

When the interface is configured with EEE and the EEE has auto-negotiated:

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

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

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show interface downshift-enable

```
show interface [<IFNNAME>|<IFRANGE>] downshift-enable
```

Description

Displays speed downshift information, including the interface speed status and configuration.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.

Examples

Showing automatic downshift information:

```
switch(config-if)# show interface downshift-enable
-----
Port          Downshift          Speed
             Enabled | Active   Status  | Config
-----
1/1/1         yes             yes     100M-FDx  auto
1/1/2         yes             no      1G         auto
1/1/3         yes             no      100M-FDx  100M-FDx
1/1/4         no              no      --         auto
```

Showing automatic downshift information on per interface:

```
switch(config-if)# show interface 1/1/2 downshift-enable
-----
Port          Downshift          Speed
             Enabled | Active   Status  | Config
-----
1/1/2         yes             no      1G         auto
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config interface

```
show running-config interface [<IFNNAME>|<IFRANGE>]
show running-config interface [lag | loopback | tunnel | vlan ] [<ID>]
```

Description

Displays active configurations of various switch interfaces.

Parameter	Description
<IFNAME>	Specifies a interface name.
<IFRANGE>	Specifies the port identifier range.
LAG	Specifies LAG interface information
LOOPBACK	Specifies loopback interface information.
TUNNEL	Specifies tunnel interface information.
VLAN	Specifies VLAN interface information.
<LAG-ID>	Specifies the LAG number. Range: 1-256.
<LOOPBACK-ID>	Specifies the LOOPBACK number. Range: 0-255.
<TUNNEL-ID>	Specifies the tunnel ID. Range: 1-255.
<VLAN-ID>	Specifies the VLAN ID. Range: 1-4094.
VXLAN	Specifies the VXLAN interface information.
<VXLAN-ID>	Specifies the VXLAN interface identifier. Default: 1.

Examples

Showing 1/1/2 interface configuration:

```
switch(config-if)# show running-config interface 1/1/2

interface 1/1/2
  no shutdown
  description DC-23
  exit
```

Showing loopback interfaces configured:

```
switch(config-if)# show running-config interface loopback

interface loopback 1
  description lb interface 1
  exit
interface loopback 2
  description lb interface 2
  exit
```

Showing loopback interfaces not configured:


```
switch(config-if)# show running-config interface loopback
```

```
No loopback interfaces configured.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	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.

Mirroring allows you to replicate all traffic arriving and/or leaving the selected system interfaces. This data can be used for collection or analysis.

The traffic replicated using mirroring can be sent to a separate interface on the same switch as the traffic source for analysis or inspection. Such a collection of interfaces and settings is called a mirror session.

A mirror session can be configured with many traffic sources but only a single output, or destination. In the initial configuration, the mirror session is disabled. You have enable the feature to start the replication.



Care must be taken in choosing the number and rates of sources to avoid over-saturating a session destination. A mirror session with multiple 10G sources can overwhelm a single 10G destination and important data may be lost.

Mirror statistics

Mirror statistics are reset for a Mirror-to-CPU session when an interface is added or removed from a LAG that is a source interface in the Mirror session and during a failover.

Classifier policies and mirroring sessions

Network traffic can be mirrored to a destination interface in two ways:

- Using a mirroring session alone.
- Using Classifier Policies with mirror actions in conjunction with a mirroring session.

Basic mirroring sessions provide coarse control over the type of traffic mirrored from a source: all received, all transmitted, or both. However, a traffic class within a Classifier Policy applied to a source can provide much finer grained control of mirrored traffic. For example, a policy can match on many different aspects of the Ethernet or IPv4 or IPv6 header information in each frame or packet received or transmitted on an interface.

The steps to configure a policy and class with a mirror action are the following:

1. Configuring a mirroring session with a destination interface.
2. Enabling the mirroring session.
3. Configuring the Classifier Policy, specifying the mirroring session ID in the mirror action.

If the packets being mirrored are received from a VLAN that is not allowed on the mirror destination, the mirrored packets would be dropped at the mirror destination interface. When the mirrored packets are dropped at the destination, the mirror output packet and byte count will increment, however the packets will not be received at the mirror destination.

The mirror destination port among the active mirror sessions must be unique. That is, if an interface is configured as a source or destination in an active mirror session, the same port cannot be used as a destination in another active mirror session.

VLAN as a source

AOS-CX allows configuration of VLAN as a mirroring source. When a VLAN source is configured in the 'rx' direction, all packets are mirrored as they are received in the switch. When a VLAN source is configured in 'tx' direction, all packets are mirrored as they are transmitted out of the switch.

More than one source VLAN can be configured in a mirror session. Each such VLAN may specify its own direction.

There is a limit of 1024 source VLANs in each direction of a given mirror session.

Same VLANs can be configured as a mirror source for multiple sessions.

Note: When changing a source VLAN in an enabled mirror session (that is, adding, changing direction, or removing), mirrored packets being transmitted out the mirror destination port from other mirror sources may be briefly interrupted during the reconfiguration.

Direction of an existing source VLAN can be updated in one of two ways:

1. Reenter the `source vlan` command with the new preferred direction.
2. Use the `no` form of the command with a direction (rx or tx) to selectively remove the specified direction. Specifying the last remaining direction for that VLAN will remove the VLAN from the configuration entirely.

For packets bridged through the switch:

If the mirror is configured in 'both' direction, two copies of packets are mirrored, otherwise one copy of the packet will be mirrored.

For routed packets:

- If the mirror is configured in the 'rx' direction, packets are mirrored in the pre-routed form with the destination MAC address as the switch address.
- If the mirror is configured in the 'tx' direction, packets are mirrored in the post-routed form with the source MAC as the switch address. Destination MAC is the nexthop gateway or station.
- If the mirror is configured in the 'both' direction, one copy of the packet will be mirrored.

Control plane packets generated by the switch's CPU are processed both in the ingress and the egress packet processing pipeline. The following are the behaviors for mirroring with VLAN as source:

- If the mirror is configured in the 'rx' or 'tx' direction, the packets are mirrored to the mirror destination.
- If the mirror is configured in the 'both' direction, two copies of the packets are mirrored to the mirror destination.

Mirroring commands

clear mirror

```
clear mirror [all | <SESSION-ID>]
```

Description

Clears the mirror statistics for all configured mirror sessions or a specified session

Parameter	Description
all	Specifies all configured sessions.
<SESSION-ID>	Specifies a numeric identifier for the session. Range: 1 to 4

Examples

Clearing mirror statistics for all configured mirror sessions:

```
switch# clear mirror all
```

Clearing mirror statistics for mirror session 1:

```
switch# clear mirror 1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

comment

```
comment <COMMENT>
no comment
```

Description

Specifies a comment for the mirroring session.

When used in mirror endpoint command context, specifies a comment for the mirror endpoint.

The `no` form of this command removes the comment.

Parameter	Description
<COMMENT>	A comment string of up to 64 characters composed of letters, numbers, underscores, dashes, spaces, and periods.

Usage

Comments are optional and can be added or removed at any time without affecting the state of the mirroring session.

Adding a comment to a session that already has a comment replaces the existing comment.

Examples

Adding a comment to a mirror session:

```
switch(config-mirror-3) # comment This Mirror will be removed during next maintenance window
```

Removing the comment from mirror session 3:

```
switch(config-mirror-3) # no comment
```

Adding a comment to a mirror endpoint:

```
switch(config-mirror-endpoint-test) # comment Monitor endpoint traffic
```

Replacing the existing comment for mirror endpoint:

```
switch(config-mirror-endpoint-test) # comment Monitor statistics on each endpoint interfaces
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror- <i><SESSION-ID></i> config-mirror-endpoint	Administrators or local user group members with execution rights for this command.

copy tcpdump-pcap

copy tcpdump-pcap *<FILE-NAME>* *<REMOTE-URL>*

Description

Saves packet capture files to external storage.

Parameter	Description
<i><FILE-NAME></i>	Specifies the packet capture file to save.
<i><REMOTE-URL></i>	Specifies the external storage to which the packet capture file will be saved.

Usage

Only four files can be saved at any point on the switch. Packet capture files are not saved after a failover or reboot. View a list of saved files using `diag utilities list-files`.

Examples

Saving my_capture_file.pcap to sftp://root@10.0.0.2/file.pcap:

```
switch# copy tcpdump-pcap my_capture_file.pcap sftp://root@10.0.0.2/file.pcap
root@10.0.0.2's password:
Connected to 10.0.0.2.
sftp > put my_capture_file.pcap file.pcap
Uploading my_capture_file.pcap to /root/file.pcap
my_capture_file.pcap          100%   156   219.8KB/s   00:00
Copied successfully.
```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6200	Manager (#)	Administrators or local user group members with execution rights for this command.

copy tshark-pcap

```
copy tshark-pcap <REMOTE-URL> [vrf <VRF-NAME>]
```

Description

Copies the tshark capture data to a file on a TFTP or SFTP server.

Parameter	Description
<REMOTE-URL>	Specifies the capture file on a remote TFTP or SFTP server. The URL syntax is: {tftp:// sftp://<USER>@} {<IP> <HOST>} [:<PORT>] [;blocksize=<SIZE>]/<FILE>
vrf <VRF-NAME>	Specifies the name of a VRF. Default: default.

Example

Copying the capture data to a file on SFTP server 10.0.0.2:

```
switch# copy tshark-pcap sftp://root@10.0.0.2/file.pcap

root@10.0.0.2's password:
Connected to 10.0.0.2.
sftp> put packets.pcap file.pcap
Uploading packets.pcap to /root/file.pcap
packets.pcap          100%   156   219.8KB/s   00:00
Copied successfully.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	Manager (#)	Administrators or local user group members with execution rights for this command.

destination cpu

```
destination cpu
no destination cpu
```

Description

The command causes the mirror session to transmit mirrored packets to the switch CPU. This destination may be configured for multiple sessions, however only one such configured session may be active at a given time.

The diagnostic utility Tshark may be used to view and capture packets transmitted to the CPU through this route. Ctrl+C must be entered to terminate a Tshark capture session. More details can be found in the *Supportability Guide*.

The `no` form of this command will immediately stops mirroring traffic to the CPU, but will not remove any sources from the mirror configuration.

Examples

Configuring a mirror session with CPU as the destination.

```
switch# config
switch(config)# mirror session 1
switch(config-mirror-1)# destination cpu
```

Removing the destination entirely.

```
switch(config-mirror-1)# no destination cpu
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror- <i><SESSION-ID></i>	Administrators or local user group members with execution rights for this command.

destination interface

```
destination interface {<INTERFACE-ID>|<LAG-NAME>}  
no destination interface {<INTERFACE-ID>|<LAG-NAME>}
```

Description

Configures the specified interface as the destination of the mirrored traffic.

The `no` form of this command immediately disables the mirroring session and removes the specified destination interface from the configuration.

Parameter	Description
<INTERFACE-ID>	Specifies a interface. Format: member/slot/port.
<LAG-NAME>	Specifies a LAG (link aggregation group) identifier.

Usage

Configuring a different destination interface in an enabled mirroring session causes all mirrored traffic to use the new destination interface. This action might cause a temporary suspension of mirrored source traffic during the reconfiguration.

Examples

Configuring a mirroring session and adding an interface as a destination:

```
switch(config)# mirror session 1  
switch(config-mirror-1)# destination interface 1/1/1
```

Replacing the existing destination with different interface:

```
switch(config-mirror-1)# destination interface 1/1/12
```

Removing a destination:

```
switch(config-mirror-1)# no destination interface 1/1/12
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror-<SESSION-ID>	Administrators or local user group members with execution rights for this command.

destination tunnel

Description

Specifies the tunnel where all mirrored traffic for the session is transmitted. Only one tunnel destination is allowed per session.

You may configure multiple mirror sessions with the same source/destination IP address pair, however, only one of those sessions sharing the same source/destination IP address pair can be enabled at a given time.

ERSPAN is not supported leaving the switch by the OOB port. If VRF management is configured for an ERSPAN session, the session will be in "mirror_err_tunnel_oob_port_not_supported" operation status.

ERSPAN is not supported leaving the switch encapsulated within another tunnel (e.g. GRE IPv4). When the path to the destination IP address will leave via a tunnel, the session will be in "tunnel_route_resolution_not_populated" operation status.



The interface/LAG used to transmit ERSPAN packets should not be a source in the same mirror session.

The `no` form of this command will cease the use of the tunnel and disable the session.

Parameter	Description
<code><TUNNEL-IPv4-ADDR></code>	Specifies the tunnel address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<code><SOURCE-IPv4-ADDR></code>	Specifies the source address in IPv4 format (x.x.x.x), where x is a decimal number from 0 to 255.
<code><DSCP-VALUE></code>	Specifies the DSCP value to be carried within the DS field of ERSPAN packet header. Range: 0 to 63. Default: 0.
<code><VRF-NAME></code>	Specifies a VRF name. Default: default.

Examples

Creating a Mirror Session and adding tunnel destination, source, dscp, and VRF:

```
switch# config
switch(config)# mirror session 1
switch(config-mirror-1)# destination tunnel 1.1.1.1 source 2.2.2.2 dscp 10 vrf default
```

Replacing the existing tunnel destination:

```
switch(config-mirror-1)# destination tunnel 11.12.13.14 source 2.2.2.2 dscp 10 vrf default
```

Replacing the existing destination with a different DSCP value:

```
switch(config-mirror-1)# destination tunnel 11.12.13.14 source 2.2.2.2 dscp 2 vrf default
```

Replacing the existing destination with a different VRF:

```
switch(config-mirror-1) # destination tunnel 11.12.13.14 source 2.2.2.2 dscp 2 vrf newvrf
```

Removing the destination:

```
switch(config-mirror-1) # no destination tunnel
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-mirror-<SESSION-ID>	Administrators or local user group members with execution rights for this command.

diagnostic

diagnostic

```
diag utilities tshark [file]
diag utilities tshark [delete-file]
```

Description

Captures packets from a mirror-to-cpu session, and save the most recent 32MB to pcap file which can then be copied and analyzed. When capturing a mirror-to-cpu session to a file, packets will not be dumped to the console.



The `diagnostic` command must be entered prior to the `diag utilities tshark` command.

Use the `delete-file` form of this command to delete the most recent capture file.

Since `file` and `delete-file` are optional, the behavior of the base command `diag utilities tshark` does **not** save anything to a file, and instead dumps the tshark session to the console until **CTRL + c** is entered.

Parameter	Description
file	Saves captured packets to a temporary file.
delete-file	Deletes the most recent captured file.

Example

Performing diagnostic:

```
switch# diagnostic

switch# diagnostic utilities tshark file
Inspecting traffic mirrored to the CPU until Ctrl-C is entered
^CEnding traffic inspection.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

diag utilities tcpdump

```
diag utilities tcpdump [command <TEXT> | delete file <FILE-NAME> | list-files |
vrf <VRF-NAME> | count <COUNT-NUM> | proto <PROTO-NUM> | host-ip <IP-ADDR> | source-ip
<IP-ADDR> | destination-ip <IP-ADDR> | host-port <PORT> | source-port <PORT> |
destination-port <PORT> | verbosity <LEVEL> | print <DATA> | ethernet-type <ETH-NUM>]
```

Description

Captures traffic received or transmitted over a network.

Parameter	Description
command <TEXT>	Captures packets based on a specified tcpdump command string.
delete file <FILE-NAME>	Deletes specified tcpdump list files.
list-files	Lists all the tcpdump capture files saved on the device.
vrf <VRF-NAME>	Captures packets on the specified VRF. If no VRF is named, the default is used.
count <COUNT-NUM>	Runs the tcpdump command until the specified number of packets are captured. Range: 1-2147483647.
proto <PROTO-NUM>	Captures packets of a particular type based on IP protocol number. Range: 0-255.
host-ip <IP-ADDR>	Captures packets matching with the source or destination IP address.
source-ip <IP-ADDR>	Captures packets from the specified IP address.
destination-ip <IP-ADDR>	Captures packets sent to the specified IP address.
host-port <PORT>	Captures packets matching with the source or destination port.

Parameter	Description
source-port <PORT>	Captures packets from the specified IP port.
destination-port <PORT>	Captures packets sent to the specified IP port.
verbosity <LEVEL>	Captures packets of the specified verbosity. Range: level1-level4. If no verbosity is specified, the default is level1.
print <DATA>	Captures the data of each packet. The maximum is 262144 bytes
ethernet-type <ETH-NUM>	Captures packets based on the particular ethernet type. Range: 0-65535.

Usage

- When using the `command` option, the only traffic captured will be packets that have been mirrored to the CPU.
- When using the `command` option, command line sanitization is performed to prevent options that may cause harm or security issues. The following options are blocked:
 - `-i/--interface`
 - `-Z`
 - `-B/--buffer-size`
 - `-C`
 - `-W`
 - `-Z/--relinquish privileges`
- Non-word operators such as "&" or "|" are not allowed. Use boolean keywords such as "and," "or," and "not."
- When using `command -r` to read a file, do not provide any directory path characters. Use `list-files` command to get the list of file names currently saved on the device, and then use those file names.
- A total of four files can be saved at any given point on the device. Packet capture files are not saved after a failover or reboot, but can be saved to external storage using the `copy tcpdump-pcap` command.

Examples

Inspecting traffic mirrored to the CPU via `tcpdump` and saving the output to `my_capture_file.pcap`:

```
switch# diag utilities tcpdump command -c 2 -x -w my_capture_file.pcap
Inspecting traffic mirrored to the CPU via tcpdump until Ctrl-C is entered.
2 packets captured
2 packets received by filter
0 packets dropped by kernel
Ending traffic capture.
```

Listing saved capture files:

```
switch# diag utilities tcpdump list-files
my_capture_file.pcap
```

Reading `my_capture_file.pcap`:

```

switch# diag utilities tcpdump command -r my_capture_file.pcap
reading from file /tmp/tcpdump/my_capture_file1.pcap, link-type EN10MB (Ethernet)
 1 11:59:34.047867 IP6 localhost.40318 > localhost.ntp: NTPv2, Reserved, length
12
    0x0000:  0000 0304 0006 0000 0000 0000 0000 0000 86dd .....
    0x0010:  600a 7e47 0014 1140 0000 0000 0000 0000  `~G...@.....
    0x0020:  0000 0000 0000 0001 0000 0000 0000 0000  .....
    0x0030:  0000 0000 0000 0001 9d7e 007b 0014 0027  .....~.{...!
    0x0040:  1601 0001 0000 0000 0000 0000  .....
 2 11:59:34.047915 IP6 localhost.ntp > localhost.40318: NTPv2, Reserved, length
12
    0x0000:  0000 0304 0006 0000 0000 0000 0000 0000 86dd .....
    0x0010:  6b8d 23c5 0014 1140 0000 0000 0000 0000  k.#....@.....
    0x0020:  0000 0000 0000 0001 0000 0000 0000 0000  .....
    0x0030:  0000 0000 0000 0001 007b 9d7e 0014 0027  .....{.~...!
    0x0040:  d681 0001 c016 0000 0000 0000  .....

```

Removing my_capture_file.pcap:

```

switch# diag utilities tcpdump delete-file my_capture_file.pcap
Successfully removed file

```

Command History

Release	Modification
10.08	Command introduced

Command Information

Platforms	Command context	Authority
6200	Manager (#)	Administrators or local user group members with execution rights for this command.

disable (mirror session)

disable

Description

Disables the mirroring session specified by the current command context.

Usage

By default, mirroring sessions are disabled.

When a mirroring session is disabled, the `show mirror` command for that session ID shows an `Admin Status` of `disable` and an `Operation Status` of `disabled`.

Example

Disabling a mirroring session:

```
switch(config)# mirror session 3
switch(config-mirror-3)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror-<SESSION-ID>	Administrators or local user group members with execution rights for this command.

enable (mirror session)

enable

Description

Enables the mirroring session for the current command context.

Usage

By default, mirroring sessions are disabled.

When a mirroring session is enabled, the `show mirror` command for that session ID shows an `Admin Status of enable` and an `Operation Status of enabled`.

If sFlow is enabled on an interface and a mirroring session specifies the same interface as the source of received traffic (the source is configured with a direction of `rx` or `both`):

- The attempt to enable the mirroring session fails and an error is returned.



When adding, removing, or changing the configuration of a source interface in an enabled mirroring session, packets from other mirror sources using the same destination interface might be interrupted.

Example

Configuring and enabling a mirroring session:

```
switch(config)# mirror session 3
switch(config-mirror-3)# source interface 1/1/2 rx
switch(config-mirror-3)# destination interface 1/1/3
switch(config-mirror-3)# comment Monitor router port ingress-only traffic
switch(config-mirror-3)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror-<SESSION-ID>	Administrators or local user group members with execution rights for this command.

mirror session

```
mirror session <SESSION-ID>
no mirror session <SESSION-ID>
```

Description

Creates a mirroring session configuration context or enters an existing mirroring session configuration context.

From this context, you can enter commands to configure and enable or disable the mirroring session.

The `no` form of this command removes an existing mirroring session from the configuration.

Parameter	Description
<SESSION-ID>	Specifies the session identifier. Range: 1 to 4

Examples

```
switch(config)# mirror session 1
switch(config-mirror-1)#

switch(config)# mirror session 3
switch(config-mirror-3)#

switch(config)# no mirror session 1
switch(config)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

show mirror

```
show mirror [<SESSION-ID>]
```

Description

Shows information about mirroring sessions. If `<SESSION-ID>` is not specified, then the command shows a summary of all configured mirroring sessions. If `<SESSION-ID>` is specified, then the command shows detailed information about the specified mirroring session.

Parameter	Description
<code><SESSION-ID></code>	Specifies the session identifier. Range: 1 to 4

Usage

Admin Status indicates the configured status. Admin Status is one of the following values:

`enable`

The mirroring session is enabled.

`disable`

The mirroring session has been configured but not yet enabled, or has been disabled.

Operation Status indicates the status of the mirroring session. Operation Status is one of the following values:

`dest_doesnt_exist`

The configured destination interface is not found in the system. The mirroring session cannot be enabled.

`destination_shutdown`

The mirroring session is enabled, but the destination interface is shut down. No traffic can be monitored.

`disabled`

The mirroring session is disabled and is not in an error condition.

`enabled`

The mirroring session is enabled.

`external/driver_error`

An internal ASIC hardware error occurred.

`hit_active_sessions_capacity`

The mirroring session could not be enabled because the maximum number of supported mirroring sessions are already enabled.

`internal_error`

An invalid parameter was passed to the ASIC software layer.

`no_dest_configured`

The mirroring session does not have a destination interface configured.

`no_name_configured`

A software error occurred. The mirroring session does not have a session ID in its configuration.

`null_mirror`

A software error occurred. The session object reference is invalid.

`out_of_memory`

The system is out of memory, reboot recommended.

`tunnel_route_resolution_not_populated`

If the destination tunnel IP address is not reachable.

`unknown_error`

An unexpected error occurred.

Examples

Showing summary information about all configured mirroring sessions:

```
switch# show mirror
ID  Admin Status  Operation Status
---  -
1   enable       enabled
2   disable      disabled
3   disable      disabled
4   enable       internal_error
```

Showing detailed information about a single mirroring session:


```

switch# show mirror 3
Mirror Session: 3
Admin Status: disable
Operation Status: disabled
Comment: Monitor router port ingress-only traffic
Source: interface 1/1/2 rx
Destination: interface 1/1/3
Output Packets: 0
Output Bytes: 0
switch#

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

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

source interface

```

source interface {<PORT-NUM> | <LAG-NAME>} [<DIRECTION>]
no source interface {<PORT-NUM> | <LAG-NAME>} [<DIRECTION>]

```

Description

Configures the specified interface (either an Ethernet port or a LAG) as a source of traffic to be mirrored. The `no` form of this command ceases mirroring traffic from the specified source interface and removes the source interface from the mirroring session configuration.

Parameter	Description
<PORT-NUM>	Specifies a physical port on the switch. Use the format <code>member/slot/port</code> (for example, <code>1/3/1</code>).
<LAG-NAME>	Specifies the identifier for the LAG (link aggregation group).
<DIRECTION>	Selects the direction of traffic to be mirrored from this source interface. There is no default for this parameter. Valid values are the following:
<code>both</code>	Mirror both transmitted and received packets.
<code>rx</code>	Mirror only received packets.
<code>tx</code>	Mirror only transmitted packets.

Usage

There is a limit of source interfaces in each direction of a given mirror session:

Switch	Source interface limit
6200	64

However, there is a practical limit to the amount of traffic that a mirror destination can transmit. For example, mirroring session with multiple 10G sources can overwhelm a single 10G destination.



When adding, removing, or changing the configuration of a source port in an enabled mirroring session, packets from other mirror sources using the same destination port might be interrupted.

Examples

Configuring a mirrored traffic source interface:

```
switch(config-mirror-1) # source interface
LAG-NAME          Enter a LAG name. For example, lag10
PORT-NUM          Enter a port number
```

Creating a mirroring session and configuring a source interface to mirror both transmitted and received packets:

```
switch(config) # mirror session 1
switch(config-mirror-1) # source interface 1/1/1 both
```

Creating a second mirroring session and configuring two source interfaces. One port mirroring only transmitted packets and the other mirroring both transmitted and received packets:

```
switch(config) # mirror session 2
switch(config-mirror-2) # source interface 1/1/3 tx
switch(config-mirror-2) # source interface 1/2/1 both
```

Removing the first source interface:

```
switch(config-mirror-2) # no source interface 1/2/3
```

Configuring a source interface to mirror received packets only:

```
switch(config-mirror-3) # source interface 1/1/2 rx
```

Configuring a source interface to mirror both transmitted and received packets:

```
switch(config-mirror-1) # source interface 1/1/1 both
```

Configuring a LAG as source interface to mirror both transmitted and received packets:

```
switch(config-mirror-4) # source interface lag1 both
```

Stopping the mirroring of received packets from a configured source interface:

```
switch(config-mirror-4) # no source interface lag1 rx
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-mirror- <i><SESSION-ID></i>	Administrators or local user group members with execution rights for this command.

source vlan

Syntax

```
source vlan <VLAN-NUM> {rx | tx | both}
no source vlan <VLAN-NUM> [rx | tx | both]
```

Description

Adds or removes VLAN as a source of traffic to be mirrored. More than one source VLAN can be configured in a mirror session. Each VLAN may specify its own direction.

The `no` version of the command ceases mirroring traffic from the specified source VLAN and removes the source from the mirror configuration.

There is a limit of 1024 source VLANs in each direction of a given mirror session. The same VLAN can be configured as a mirror source for multiple sessions.

Command context

```
config
```

Parameters

<VLAN-NUM>

Configured VLAN number.

`rx`

Mirror only received traffic.

`tx`

Mirror only transmitted traffic.

`both`

Mirror both received and transmitted traffic.

Authority

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

Example

Create a mirror session and add VLAN 10 as a source of traffic in both directions on that port.

```
switch(config)# mirror session 1  
switch(config-mirror-1)# source vlan 10 both
```

Create a second mirror session and add VLAN 10 as a transmit sources of traffic and VLAN 20 in both receive and transmit directions.

```
switch(config)# mirror session 2  
switch(config-mirror-2)# source vlan 10 tx  
switch(config-mirror-2)# source vlan 20 both
```

Reconfigure the source in session 2 to be receive only by respecifying the source interface configuration.

```
switch(config-mirror-2)# source vlan 10 rx
```

From the second session, remove the first source interface entirely and remove the transmit direction from the other so that mirroring only occurs in the receive direction.

```
switch(config-mirror-2)# no source vlan 10  
switch(config-mirror-2)# no source vlan 20 tx
```

Message received when trying to add more than 1024 mirror source VLANs

```
switch(config-mirror-2)# source vlan 2000 rx  
The maximum number of source VLANs per mirror session is 1024 in each direction
```

Configuring SNMP: Refer to the *SNMP/MIB Guide* for information on how to add SNMP so a device can be monitored from a network management system (NMS).

Configuring an SNMP trap receiver: Refer to the *SNMP/MIB Guide* and specific information about the `show snmp trap` command to enable SNMP traps.

- The Power-over-Ethernet (PoE) subsystem manages power supplied to devices using standard Ethernet data cables. A Power Sourcing Equipment (PSE) supplies DC power as well as Ethernet connectivity to a Powered Device (PD) using a standard Ethernet cable. The maximum current depends on the PD Requested Class.
- A PoE subsystem contains two parts : a PSE and PD. A Power Sourcing Equipment (PSE) is a device that provides power through a standard Ethernet cable. A PoE capable switch functions as PSE. All Aruba PoE switches are considered as PSEs. A PD is a device powered by a PSE. Examples of PD are VoIP phones, Wireless APs, and IP cameras.
- When a PD or any network cable is connected to a PSE port, the PSE applies a detection voltage and measures the resistance value of the PD. If resistance is within IEEE 802.3 standard values (23 - 26k ohm), the connected device is treated as PD and classification begins. For legacy devices to be detected, you must enable prestandard detection on the switch.
- PDs are divided into different types and classes based on PD power requirements. The power supplied by the PSE is higher than the power PD draws to accommodate for the line losses that can result with the use of the standard maximum length cable(100m).
 - Type 1: PSE can supply maximum of 15.4W, and PD can draw a maximum of 13W.
 - Type 2: PSE can supply maximum of 30W, and PD can draw a maximum of 25.5W.
 - Type 3: PSE can supply maximum of 60W, and PD can draw a maximum of 51W.
 - Type 4: PSE can supply maximum of 90W, and PD can draw a maximum of 71W.
- Classes of PD:
 - Class 0: Type1 PD, it can draw a maximum of 13W.
 - Class 1: Type1 PD, it can draw a maximum of 3.84W.
 - Class 2: Type1 PD, it can draw a maximum of 6.49W.
 - Class 3: Type1 PD, it can draw a maximum of 13W.
 - Class 4: Type2 PD, it can draw a maximum of 25.5W.
 - Class 5: Type3 PD, it can draw a maximum of 40W.
 - Class 6: Type3 PD, it can draw a maximum of 51W.
 - Class 7: Type4 PD, it can draw a maximum of 62W.
 - Class 8: Type4 PD, it can draw a maximum of 71.3W.
- IEEE 802.3bt introduced 4-Pair PoE as a means of supplying higher power to PDs that need more than the current 25.5W supplied by IEEE 802.3at. To increase the available power without damaging the Ethernet cable, the standard introduced the ability to use all four pairs within the Ethernet cable instead of the two pairs used by previous standards (802.3at, 802.3af).
- Supported protocols:
 - Compatibility with IEEE 802.3af, 802.3at, 802.3bt and prestandard.
 - Long first class event supported on Type 3-4 PSE.
 - Support for Single Signature (SS) Type 0-6 and Dual Signature (DS) Type 0-4 PDs.
 - Multi-Event classification permits mutual ID of SS Class 0-6 and DS Class 0-4.

- Support LLDP Data Link Layer (DLL) Type 1-2 extension 12-octet TLV and Type 3-4 extension 29-octet TLV.
- Default PSE assigned class delivers the maximum PSE capable power at initial power up based on PD requested class.
- Always-on PoE is a feature that provides the ability for a switch to continue to provide power across user initiated reboots through software. Always-on PoE is enabled by default and no additional configuration is needed.



PDs only remain powered, no data transfer or PoE power negotiation can occur until the switch has completely booted up and in normal operation. PD faults occurring prior to full switch boot up will result in PoE power removal and restart the detection process only after switch returns to normal operation.

PoE commands

All PoE configuration commands except `threshold` configuration and `always-on poe` configuration are entered at the `config-if` context. The PoE threshold command is used at the system level whereas the `always-on poe` and `power-over-ethernet quick-poe` commands are set at the slot level. These commands can only be configured in the global configuration context.

lldp dot3 poe

```
lldp dot3 poe
no lldp dot3 poe
```

Description

Enables 802.3 TLV list in LLDP to advertise for Power over Ethernet Data Link Layer Classification. LLDP dot3 TLV is by default enabled for PoE.

The `no` form of this command disables 802.3 TLV list in LLDP.

Examples

Enabling 802.3 TLV list in LLDP:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp dot3 poe
```

Disabling 802.3 TLV list in LLDP:

```
switch(config-if)# no lldp dot3 poe
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

lldp med poe

```
lldp med poe [priority-override]
no lldp med poe [priority-override]
```

Description

Enables MED TLV list in LLDP to advertise for Power over Ethernet Data Link Layer Classification. Also enables the lldp-MED TLV priority to override user configured port priority for Power over Ethernet. When both dot3 and MED are enabled, dot 3 will take precedence. MED TLV is by default enabled for PoE. Priority over-ride is by default disabled.

The `no` form of this command disables MED TLV list in LLDP.

Parameter	Description
[priority-override]	System defined name of the interface.

Examples

Enabling and disabling LLDP MED PoE:

```
switch(config)# interface 1/1/1
switch(config-if)# lldp med poe
switch(config-if)# no lldp med poe
```

Enabling and disabling LLDP MED PoE priority override:

```
switch(config-if)# lldp med poe priority-override
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet

```
power-over-ethernet
no power-over-ethernet
```

Description

Enables per-interface power distribution. Per-port power is enabled by default with priority low. PoE cannot be disabled for individual ports when Quick PoE is enabled for the entire switch or line module. The `no` form of this command disables per-interface power distribution.

Examples

Enabling per-interface power distribution:

```
switch(config)# interface 1/1/1  
switch(config-if)# power-over-ethernet
```

Disabling per-interface power distribution:

```
switch(config-if)# no power-over-ethernet
```

Showing Quick PoE enabled:

```
switch(config-if)# power-over-ethernet quick-poe 1/1  
switch(config-if)# interface 1/1/1  
switch(config-if)# no power-over-ethernet  
Interface PoE cannot be disabled when Quick PoE is enabled.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet allocate-by

```
power-over-ethernet allocate-by {usage | class}  
no power-over-ethernet allocate-by {usage | class}
```

Description

Configures the power allocation method. Power allocation method is initially based on usage. PSE Allocated power value will change to LLDP negotiated power if and when LLDP exchange takes place between PSE and PD. When there is no LLDP negotiation, PSE Allocated Power Value will be the actual instantaneous power draw and reserve power based on actual consumption. In allocate-by class, power allocation is based on PD requested class and PSE allocated power value will be the LLDP negotiated power when LLDP exchange takes place between PSE and PD. When there is no LLDP negotiation, PSE Allocate Power will be based on PD class. Reserve power is based on PD Class. By default, power allocation is by usage.

The `no` form of this command resets the action to default.

Examples

Configuring the power allocation method:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet allocate-by usage
switch(config-if)# power-over-ethernet allocate-by class
```

Resetting power allocation method:

```
switch(config-if)# no power-over-ethernet allocate-by class
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet always-on

```
power-over-ethernet always-on <MODULE-ID>
no power-over-ethernet always-on <MODULE-ID>
```

Description

Always-on PoE is a feature that provides the ability to the switch to continue to provide power across a soft reboot. It is applicable only to the interfaces which were connected and delivering before the soft reboot. Also, power will not be delivered if power to the switch is interrupted. This command enables or disables the always-on PoE feature at the switch or the slot level. By default, always-on PoE is enabled at the switch or the slot level.

The `no` form of this command disables power distribution on soft reboot.

Parameter	Description
<MODULE-ID>	Module number to apply always-on PoE configuration.

Examples

Enabling per-interface power distribution:

```
switch(config)# power-over-ethernet always-on 1/1
```

Disabling per-interface power distribution:

```
switch(config)# no power-over-ethernet always-on 1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Administrators or local user group members with execution rights for this command.

power-over-ethernet assigned-class

```
power-over-ethernet assigned-class {3 | 4 | 6}  
no power-over-ethernet assigned-class
```

Description

Limit PoE power based on the assigned class. When an user assigns a maximum class to an interface, the PSE will limit the maximum power delivered to the PD up to a total power draw not exceeding the PSE assigned-class power. Power demotion occurs when a PD requested class is higher than the PSE assigned class, permitting the PD to receive power and operate in a reduced power mode. PoE ports cannot set an assigned class when Quick PoE is enabled on the subsystem. The default assigned class is 4 for 2-pair capable PSE and 6 for 4-pair capable PSE.

The `no` form of this command resets the action to default.

Examples

Setting PoE assigned class:

```
switch(config)# interface 1/1/1  
switch(config-if)# power-over-ethernet assigned-class 4
```

Resetting PoE assigned class to default:

```
switch(config-if)# no power-over-ethernet assigned-class 4
```

Showing Quick PoE enabled:

```
switch(config)# power-over-ethernet quick-poe 1/1  
switch(config)# interface 1/1/1  
switch(config)# power-over-ethernet assigned-class 4  
Interface assigned class cannot be configured when Quick PoE is enabled.
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet pre-std-detect

```
power-over-ethernet pre-std-detect
no power-over-ethernet pre-std-detect
```

Description

Before IEEE 802.3 released the first Power over Ethernet standard (802.3af), vendors had shipped PoE capable switches and PD's. As we are backward compatible Aruba will support both IEEE standard and pre-standard 802.3af Power over Ethernet PD's concurrently. This CLI allows the user to enable or disable pre-802.3af-standard device detection and powering on the specific port. When pre-std-detect is enabled, power will be delivered on PairA only. Default is disabled.

The `no` form of this command resets the action to default.

Examples

Enabling standard device detection:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet pre-std-detect
```

Disabling standard device detection:

```
switch(config-if)# no power-over-ethernet pre-std-detect
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet priority

```
power-over-ethernet priority {critical | high | low}
```

```
no power-over-ethernet priority {critical | high | low}
```

Description

Sets PoE priority for an interface. Specifying critical, high, or low indicates the priority of the interface in the event of power over-subscription. Within the same priority level, higher power-priority line-module ports have higher precedence. With same PoE priority and same line-module priority, lower numbered line-module ports have higher precedence. Per-interface PoE priority is low by default.

The `no` form of this command resets the priority to default PoE priority "low".

Examples

Configuring PoE priority:

```
switch(config)# interface 1/1/1
switch(config-if)# power-over-ethernet priority critical
switch(config-if)# power-over-ethernet priority high
```

Resetting the PoE priority to default:

```
switch(config-if)# no power-over-ethernet priority high
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet quick-poe

```
power-over-ethernet quick-poe <MODULE-ID>
no power-over-ethernet
```

Description

Quick PoE is a feature that provides the ability for the switch to provide power to the connected powered device as soon as switch goes through cold reboot. When quick PoE is enabled on the subsystem PoE port disablement and PD demotion is not allowed. Also quick PoE enablement is not allowed if any of the port is disabled on the subsystem. User should not over-subscribe the PoE power when quick PoE is enabled. Quick PoE saved configuration will work irrespective of the configuration change at reboot.

Enables quick PoE feature on the switch or the subsystem level. By default, quick-PoE is disabled for the subsystem.

The `no` form of this command disables quick PoE.

Parameter	Description
<MODULE-ID>	Specifies module number for quick PoE configuration .

Examples

Enabling and disabling quick PoE:

```
switch(config)# power-over-ethernet quick-poe 1/2
switch(config)# no power-over-ethernet quick-poe 1/2
```

```
switch(config-if)# power-over-ethernet quick-poe 1/1
PoE must be enabled on all interfaces before enabling Quick PoE
```

```
switch(config-if)# power-over-ethernet quick-poe 1/3
All interfaces must use the default assigned class before enabling Quick PoE
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

power-over-ethernet threshold

```
power-over-ethernet threshold <PERCENTAGE>
no power-over-ethernet threshold <PERCENTAGE>
```

Description

Sets the threshold at which the system will send an excess power consumption notification trap. Default value is 80 percentage.

The `no` form of this command resets the action to default.

Parameter	Description
<PERCENTAGE>	Excess power consumption trap threshold. Range 1-99.

Examples

Setting the power-over-ethernet threshold:

```
switch(config)# power-over-ethernet threshold 75
```

Resetting the power-over-ethernet threshold to default:

```
switch(config-if) # no power-over-ethernet threshold 75
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config	Administrators or local user group members with execution rights for this command.

power-over-ethernet trap

```
power-over-ethernet trap  
no power-over-ethernet trap
```

Description

This command enables/disables the SNMP trap generation for PoE related events at system level. PoE trap generation is enabled by default.

The `no` form of this command resets the priority to default PoE priority "low".

Examples

Enabling SNMP trap generation for PoE:

```
switch(config) # power-over-ethernet trap
```

Disabling SNMP trap generation for PoE:

```
switch(config-if) # no power-over-ethernet trap
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	config-if	Administrators or local user group members with execution rights for this command.

show lldp local

show lldp local-device [<INTERFACE-ID>]

Description

Displays information advertised by the switch if the LLDP feature is enabled by user.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: member/slot/port

Examples

Showing LLDP local device:

```
switch# show lldp local-device 1/1/10
Local Port Data
=====

Port-ID           : 1/1/10
Port-Desc         : "1/1/10"
Port VLAN ID     : 0

PoE Plus Information

PoE Device Type   : Type 2 PSE
Power Source      : Primary
Power Priority     : low
PSE Allocated Power: 25.0 W
PD Requested Power : 25.0 W
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show lldp neighbor

show lldp neighbor [<INTERFACE-ID>]

Description

Displays detailed information about a particular neighbor connected to a particular interface.

Parameter	Description
<INTERFACE-ID>	Specifies an interface. Format: member/slot/port

Examples

Showing LLDP neighbor information when there is only one neighbor:

```
switch# show lldp neighbor-info 1/1/10

Port : 1/1/10
Neighbor Entries : 1
Neighbor Entries Deleted : 0
Neighbor Entries Dropped : 0
Neighbor Entries Aged-Out : 0
Neighbor Chassis-Name : 84:d4:7e:ce:5d:68
Neighbor Chassis-Description : ArubaOS (MODEL: 325), Version Aruba IAP
Neighbor Chassis-ID : 84:d4:7e:ce:5d:68
Neighbor Management-Address : 169.254.41.250
Chassis Capabilities Available : Bridge, WLAN
Chassis Capabilities Enabled :
Neighbor Port-ID : 84:d4:7e:ce:5d:68
Neighbor Port-Desc : eth0
TTL : 120
Neighbor Port VLAN ID :
Neighbor PoEplus information : DOT3
Neighbor Device Type : TYPE2 PD
Neighbor Power Priority : Unkown
Neighbor Power Source : Primary
Neighbor Power Requested : 25.0 W
Neighbor Power Allocated : 0.0 W
Neighbor Power Supported : No
Neighbor Power Enabled : No
Neighbor Power Class : 5
Neighbor Power Paircontrol : No
Neighbor Power Pairs : SIGNAL
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show power-over-ethernet

```
show power-over-ethernet [member <MEMBER-ID>] [brief]
```

Description

Displays the status information of the full system.

Parameter	Description
<MEMBER-ID>	Displays the detailed status of given member.
<IFNAME>	Display the detailed status of given port.
brief	Display the brief status of all ports or the given port.

Examples

Showing sample output for show power-over-ethernet on standalone box with VSF capability:

```
switch# show power-over-ethernet

System Power Status for member 1

Configured Power Status      : No redundancy
Operational Power Status     : No redundancy
Total Available Power        : 740 W
Total Failover Pwr Avl       : 0 W
Total Redundancy Power       : 0 W
Total Power Drawn            : 0 W +/- 6W
Total Power Reserved         : 0 W
Total Remaining Power        : 740 W
Trap Threshold               : 80 %
Trap Enabled                 : Yes
Always-on PoE Enabled        : 1/1
Quick PoE Enabled           : None
```

```
Internal Power
  Total Power
  PS      (Watts)      Status
  -----
  1       0            Absent
  2      740           Ok
```

```
System Power Status for member 2

Configured Power Status      : No redundancy
Operational Power Status     : No redundancy
Total Available Power        : 600 W
Total Failover Pwr Avl       : 0 W
Total Redundancy Power       : 0 W
Total Power Drawn            : 0 W +/- 6W
Total Power Reserved         : 0 W
Total Remaining Power        : 600 W
Trap Threshold               : 80 %
Trap Enabled                 : Yes
Always-on PoE Enabled        : None
Quick PoE Enabled           : None
```

```
Internal Power
  Total Power
  PS      (Watts)      Status
  -----
  1       0            Absent
  2      600           Ok
```

Showing sample output for power-over-ethernet member:

```

switch# show power-over-ethernet member 1

System Power Status for member 1

Configured Power Status      : No redundancy
Operational Power Status     : No redundancy
Total Available Power        : 740 W
Total Failover Pwr Avl       : 0 W
Total Redundancy Power       : 0 W
Total Power Drawn            : 0 W +/- 6W
Total Power Reserved         : 0 W
Total Remaining Power        : 740 W
Trap Threshold               : 80 %
Trap Enabled                 : No
Always-on PoE Enabled        : 1/1
Quick PoE Enabled           : 1/1

```

```

Internal Power
Total Power
PS      (Watts)      Status
-----
1       0            Absent
2       740          Ok

```

Showing sample output for power-over-ethernet brief in a VSF stack:

```

switch# show power-over-ethernet brief

Status and Configuration Information for PoE

Member 1 Power Status
  Available: 370 W Reserved: 55.60 W Remaining: 314.40 W
  Always-on PoE Enabled: 1/1
  Quick PoE Enabled: None

PoE      Pwr Power   Pre-std Alloc PSE Pwr PD Pwr PoE Port   PD   Cls Type
Port     En  Priority Detect  Act  Rsrvd Draw  Status Sign      Type
-----
1/1/1   Yes Low    Off    Class 0.0 W  0.0 W Denied  None  4    2
1/1/2   Yes Critical Off    Usage 1.6 W  1.5 W Delivering* Single 0    1
1/1/3   Yes High   Off    Class 54.0 W 25.5 W Delivering**^ Dual  1/3 3
1/1/4   No  Low     On     Usage 0.0 W  0.0 W Disabled None  N/A  N/A

Member 2 Power Status
  Available: 600 W Reserved: 0.00 W Remaining: 600 W
  Always-on PoE Enabled: None
  Quick PoE Enabled: None

PoE      Pwr Power   Pre-std Alloc PSE Pwr PD Pwr PoE Port   PD   Cls Type
Port     En  Priority Detect  Act  Rsrvd Draw  Status Sign      Type
-----
2/1/1   Yes Low    Off    Class 0.0 W  0.0 W Searching None  N/A  N/A
2/1/2   Yes Critical Off    Usage 0.0 W  0.0 W Searching None  N/A  N/A
2/1/3   Yes High   Off    Class 0.0 W  0.0 W Searching None  N/A  N/A
2/1/4   No  Low     On     Usage 0.0 W  0.0 W Disabled None  N/A  N/A

*This port may go down in the event of a PSU failure.
^This port is power demoted due to user config or power availability.

```

Showing sample output for power-over-ethernet brief per-port:

```

switch# show power-over-ethernet 1/1/1 brief

Status and Configuration Information for port 1/1/1

Member 1Power Status
  Available: 370 W Reserved: 55.60 W Remaining: 314.40 W
  Always-on PoE Enabled: 1/1
PoE      Pwr Power    Pre-std Alloc PSE Pwr PD Pwr PoE Port    PD    Cls Type
Port     En  Priority Detect   Act  Rsrvd Draw  Status Sign  --- ----
-----
1/1/1    Yes Low         Off    Class 0.0 W  0.0 W Denied None  4   2

```

Showing sample output for power-over-ethernet brief for interface range:
For 6300 Switch series:

```

switch# show power-over-ethernet 1/1/1-1/1/2 brief

Status and Configuration Information for port 1/1/1-1/1/2

Member 1Power Status
  Available: 370 W Reserved: 55.60 W Remaining: 314.40 W
  Always-on PoE Enabled: 1/1
  Quick PoE Enabled: None
PoE      Pwr Power    Pre-std Alloc PSE Pwr PD Pwr PoE Port    PD    Cls Type
Port     En  Priority Detect   Act  Rsrvd Draw  Status Sign  --- ----
-----
1/1/1    Yes Low         Off    Class 0.0 W  0.0 W Denied None  4   2
1/1/2    Yes Critical Off     Usage 1.6 W  1.5 W Delivering* Single 0   1

```

Showing sample output for power-over-ethernet for a missing line card:

```

switch# show power-over-ethernet 1/3 brief

Module 1/3 is not physically present.

```

Showing sample output for power-over-ethernet brief for a missing member:

```

switch# show power-over-ethernet member 3 brief

Member 3 is not physically present.

```

Showing sample output for power-over-ethernet port when physical interface is not present:

```

switch# show power-over-ethernet 2/1/1

Interface 2/1/1 is not present.

```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

You can manage and monitor the AOS-CX switch through Aruba AirWave. The following benefits and functions include:

- Configuration (partial configuration)
- Device topology
- Immediate and historical trend reports
- Monitoring of the device and user connected to the network.
- Network discovery
- Syslogs and trap receiver

For information about which versions of Aruba AirWave support AOS-CX, see the *AOS-CX Release Notes*.

SNMP support and AirWave

For AirWave to discover and monitor the switch, you must:

- Enable the SNMP services on the switch.
- Configure the SNMP agent to use the SNMP version supported by the management station.

SNMP on the switch

The switch provides SNMP services through the management channel and the data interfaces. Functionality, such as device discovery from NMS, syslog and trap forwarding, can be any channel configured by you.

Although the SNMP server can be enabled on both VRFs (`mgmt` and `default`), only one instance of SNMP can be running. The highest priority is on the `default` VRF.

For example, assume that SNMP is first enabled on the `mgmt` VRF (`snmp-server vrf mgmt`). Then, SNMP is enabled on the `default` VRF (`snmp-server vrf default`) without disabling SNMP on the `mgmt` (using an equivalent `no` form of the command). The `show running-config` command displays both `snmp-server vrf` commands; however, the SNMP instance is running only on the `default` VRF (highest priority).

```
switch# config
switch(config)# snmp-server vrf mgmt
switch(config)# snmp-server vrf default
switch(config)# show running-config
Current configuration:
!
!Version AOS-CX Virtual.10.01.
led locator on
!
!
!
snmp-server vrf default
snmp-server vrf mgmt
```

!
...

Supported features with AirWave and the AOS-CX switch

AirWave supports the following features with the AOS-CX switch:

Device management	Device discovery using SNMPv2C and SNMPv3
	Device dashboards
Monitoring management	Device health attributes (device status/reachability)
	Interface and VLAN management
	Initiates an SSH connection from Aruba AirWave to AOS-CX so that the device outputs from the AOS-CX CLI can be displayed in the Aruba AirWave user interface.
	Firmware versions
	Displays neighbor devices connected to AOS-CX switches
	Device topology
Configuration management	Partial configuration
Alarm management	Alarm triggers (device and interface up/down, new device discoveries, custom event triggers)
	Syslogs and traps
Report management	Device inventory, interface utilization, and device reachability reports
	Summary report of device model, firmware, and boot loader version

Configuring the AOS-CX switch to be monitored by AirWave

Prerequisites

Aruba AirWave is active on the network.

Procedure

1. Enable SNMP on the switch by entering the `snmp-server vrf mgmt` command.

```
switch(config)# snmp-server vrf mgmt  
switch(config)# snmp-server vrf default
```

2. Configure the SNMPv2C community to public by entering the `snmp-server community public` command. In this instance, `public` is a read-only community string.

```
switch(config)# snmp-server community public
```

3. The community-string is used by SNMPv1 and SNMPv2C for unencrypted authentication. SNMPv3 lets you encrypt the authentication mechanism. To enable SNMPv3, enter the `snmpv3 user` and `snmpv3 context` commands.

```
switch(config)# snmpv3 user Admin auth sha auth-pass ciphertext
AQBapZHf2d20GYr/xcGUzYzm0zjNf/4VKHtSqbNImqtfYbJYCgAAALkGFJVcSp3nZ3o=
priv des priv-pass ciphertext
AQBapb0H2poBQKXPoVsC9L9qzZyfJQnzR7hmTr7LGsOsI7K3CgAAAKP98Rq2jfTrFwQ=
switch(config)# snmpv3 context Admin
```

For discovering devices in AirWave through the SNMPv3 community, the SNMPv3 context name is not mandatory. Devices can still be discovered in Aruba AirWave without the SNMPv3 context name.

4. Enter the `logging` command for enabling syslog forwarding to a remote syslog server, such as AirWave:

```
switch(config)# logging 10.0.10.2 severity debug
```

5. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Enable SNMP traps by entering the `snmp-server host` command:

```
switch(config)# snmp-server host 10.10.10.10 trap version v2c vrf default
```

SNMP traps cannot be forwarded from AOS-CX 10.00 switches that have the VRF configured as `mgmt`. Later versions of AOS-CX support SNMP trap forwarding even when the VRF is configured as `default` or `mgmt`.

6. For information on how to add a device for monitoring in the Aruba AirWave user interface, see the documentation for Aruba AirWave.

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
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.